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
«Основы управления информационной безопасностью»

Направление подготовки – 10.03.01 «Информационная безопасность»
Направленность (профиль) – «Техническая защита информации»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций**:**

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.	ОПК-5. ОУИБ. Способен применять нормативные правовые акты, нормативные и методические документы при организации управления информационной безопасностью на объектах информатизации	**Знания:** структуру и основное содержание национальных стандартов в области информационной безопасности (серий ГОСТ Р ИСО/МЭК 27000 и ГОСТ Р ИСО/МЭК 1333, ГОСТ Р ИСО/МЭК ТО 18044-2007 и др.); структуру и основное содержание нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю по защите информации на объектах информатизации; цели и задачи управления информационной безопасностью (ИБ); роль концепции ИБ в процессах управления информационной безопасности. Основные (обязательные, типовые) положения концепции ИБ; понятие политики ИБ. Основные требования, принципы и подходы к разработке политики ИБ; структуру политики ИБ (организационные и технические компоненты), область действия и цикл жизни политики безопасности, непрерывность и цикличность развития политики безопасности; процесс разработки политики ИБ, организационные аспекты (постановка задачи, мотивация, обеспечение и контроль) процесса разработки; практические правила управления ИБ; цели и задачи аудит ИБ. Объекты аудита ИБ. Виды аудита ИБ. Методы аудита. Принципы проведения аудита. Структура отчёта о результатах аудита ИБ.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		Умения: разрабатывать проекты концепций информационной безопасности организации; разрабатывать модели угроз безопасности информации; разрабатывать организационно распорядительные документы по защите автоматизированной системы от несанкционированного доступа к информации. **Опыт практической деятельности:** разработки проектов технических заданий на создание СЗИ ОИ.
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.ОУИБ. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**Знания:** структуру и основное содержание нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю по защите информации на объектах информатизации; цели и задачи защиты информации в организации. Система защиты информации (СЗИ) организации. Порядок создания и ввода в эксплуатацию СЗИ. предпроектное специальное обследование объектов информатизации (ОИ); модели угроз безопасности информации; содержание и порядок разработки технического задания на создание СЗИ ОИ; порядок разработки (проектирования) СЗИ. Стадия создания СЗИ (эскизный проект; технический проект; рабочая документация); состав и содержание технического проекта СЗИ; порядок ввод СЗИ ОИ в эксплуатацию; организацию аттестации ОИ по требо-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		ваниям по безопасности информации; организацию управления СЗИ. **Умения:** проводить предпроектное специальное обследование объекта информатизации; разрабатывать модели угроз безопасности информации; разрабатывать проекты технических заданий на создание СЗИ ОИ; разрабатывать технические паспорта на ОИ; разрабатывать организационно распорядительные документы по защите автоматизированной системы от несанкционированного доступа к информации. **Опыт практической деятельности:** разработки проектов технических заданий на создание СЗИ ОИ.
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты		**Знания:** структуру и основное содержание национальных стандартов в области информационной безопасности (серий ГОСТ Р ИСО/МЭК 27000 и ГОСТ Р ИСО/МЭК 1333, ГОСТ Р ИСО/МЭК ТО 18044-2007 и др.); структуру и основное содержание нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю по защите информации на объектах информатизации; цели и задачи управления информационной безопасностью (ИБ); роль концепции ИБ в процессах управления информационной безопасности. Основные (обязательные, типовые) положения концепции ИБ; понятие политики ИБ. Основные требования, принципы и подходы к разработке политики ИБ;

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		структуру политики ИБ (организационные и технические компоненты), область действия и цикл жизни политики безопасности, непрерывность и цикличность развития политики безопасности; процесс разработки политики ИБ, организационные аспекты (постановка задачи, мотивация, обеспечение и контроль) процесса разработки; практические правила управления ИБ; цели и задачи аудит ИБ. Объекты аудита ИБ. Виды аудита ИБ. Методы аудита. Принципы проведения аудита. Структура отчёта о результатах аудита ИБ; организацию и обеспечение режима секретности (конфиденциальности) организации; организацию контроля состояния защиты информации на предприятии. **Умения:** разрабатывать проекты концепций информационной безопасности организации; разрабатывать модели угроз безопасности информации; разрабатывать проекты технических заданий на создание СЗИ ОИ; разрабатывать технические паспорта на ОИ; разрабатывать организационно распорядительные документы по защите автоматизированной системы от несанкционированного доступа к информации. **Опыт практической деятельности:** разработки проектов технических заданий на создание СЗИ ОИ.
ОПК-12. Способен проводить подготовку исходных данных для проектирования	ОПК-12.ОУИБ. Способен проводить подготовку исходных данных для проектирования	**Знания:** структуру и основное содержание нормативных и методических документов Федеральной службы безопасности Российской Федерации, Феде-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	подсистем, средств обеспечения защиты информации	ральной службы по техническому и экспортному контролю по защите информации на объектах информатизации; цели и задачи защиты информации в организации. Система защиты информации (СЗИ) организации; порядок создания и ввода в эксплуатацию СЗИ; предпроектное специальное обследование объектов информатизации (ОИ); модели угроз безопасности информации; содержание и порядок разработки технического задания на создание СЗИ ОИ. **Умения:** проводить предпроектное специальное обследование объекта информатизации; разрабатывать модели угроз безопасности информации; разрабатывать проекты технических заданий на создание СЗИ ОИ. **Опыт практической деятельности:** разработки проектов технических заданий на создание СЗИ ОИ.

В результате изучения дисциплины студент должен:

Знать:

структуру и основное содержание национальных стандартов в области информационной безопасности (серий ГОСТ Р ИСО/МЭК 27000 и ГОСТ Р ИСО/МЭК 1333, ГОСТ Р ИСО/МЭК ТО 18044-2007 и др.);

структуру и основное содержание нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю по защите информации на объектах информатизации;

цели и задачи управления информационной безопасностью (ИБ);

роль концепции ИБ в процессах управления информационной безопасности. Основные (обязательные, типовые) положения концепции ИБ;

понятие политики ИБ. Основные требования, принципы и подходы к разработке политики ИБ;

структуру политики ИБ (организационные и технические компоненты), область действия и цикл жизни политики безопасности, непрерывность и цикличность развития полити-

ки безопасности;

процесс разработки политики ИБ, организационные аспекты (постановка задачи, мотивация, обеспечение и контроль) процесса разработки;

практические правила управления ИБ;

цели и задачи аудит ИБ. Объекты аудита ИБ. Виды аудита ИБ. Методы аудита. Принципы проведения аудита. Структура отчёта о результатах аудита ИБ;

цели и задачи защиты информации в организации. Система защиты информации (СЗИ) организации. Порядок создания и ввода в эксплуатацию СЗИ.

предпроектное специальное обследование объектов информатизации (ОИ);

модели угроз безопасности информации;

содержание и порядок разработки технического задания на создание СЗИ ОИ;

порядок разработки (проектирования) СЗИ. Стадия создания СЗИ (эскизный проект; технический проект; рабочая документация);

состав и содержание технического проекта СЗИ;

порядок ввод СЗИ ОИ в эксплуатацию;

организацию аттестации ОИ по требованиям по безопасности информации;

организацию управления СЗИ;

организацию и обеспечение режима секретности (конфиденциальности) организации;

организацию контроля состояния защиты информации на предприятии.

Уметь:

проводить предпроектное специальное обследование объекта информатизации;

разрабатывать проекты концепций информационной безопасности» организации;

разрабатывать модели угроз безопасности информации;

разрабатывать проекты технических заданий на создание СЗИ ОИ;

разрабатывать технические паспорта на ОИ;

разрабатывать организационно распорядительные документы по защите автоматизированной системы от несанкционированного доступа к информации.

Иметь опыт практической деятельности:

разработки проектов технических заданий на создание СЗИ ОИ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы управления информационной безопасностью» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 4-м курсе в 7-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении следующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Защита информации от утечки по техническим каналам», «Защита информации от несанкционированного доступа», «Программно-аппаратные средства защиты», «Физическая защита объектов информатизации».

Знания и умения, полученные в результате изучения дисциплины, используются при изучении дисциплины «Проектирование систем защиты объектов информатизации (деловая

игра)», а также при прохождении учебной и производственной практик 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 курсовой работы (проекта)	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации			
4	7	5	180	80	32	-	32	16	64	28	Экз. (36), КР

* 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	Лабораторные работы	Практические занятия	Групповые консультации			
1. Основы управления информационной безопасностью	14	-	16	8	18	-	Компьютерный тест (РК-1). Зачет по ПЗ № 2 и 3
2. Организация защиты информации в организации	18	-	16	8	46	28	Компьютерный тест (РК-2). Зачет по ПЗ № 5-8. Защита курсового проекта

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1	2	**Цели и задачи управления информационной безопасностью.** Цели и задачи управления информационной безопасностью (ИБ), эволюция подходов к управлению безопасностью - реактивный («продуктовый»), системно-сервисный, интеграционный, инфраструктурный, архитектурный. Управление адекватностью и управление рисками. Система управления информационной безопасностью (структура, взаимосвязь основных процессов управления и их основное содержание).
	2	2	**Стандартизация управления информационной безопасностью.** Классификация основных международных стандартов в области ИБ. Назначение, структура и основное содержание основных международных стандартов в области ИБ, особенности применения международных стандартов в области ИБ в РФ.
	3	2	**Стандартизация управления информационной безопасностью.** Классификация основных национальных стандартов в области ИБ. Назначение, структура и основное содержание основных национальных стандартов в области ИБ (серий ГОСТ Р ИСО/МЭК 27000 и ГОСТ Р ИСО/МЭК 1333, ГОСТ Р ИСО/МЭК ТО 18044-2007 и др.), особенности применения национальных стандартов в области ИБ.
	4	2	**Концепция информационной безопасности организации.** Роль концепции в процессах управления информационной безопасности. Принципы фундаментальности и декларативности при создании концепции ИБ как системы взглядов на обеспечение информационной безопасности. Основные (обязательные, типовые) положения концепции информационной безопасности.
	5	2	**Политика информационной безопасности.** Понятие политики информационной безопасности. Основные требования, принципы и подходы к разработке политики информационной безопасности. Структура политики информационной безопасности (организационные и технические компоненты), область действия и цикл жизни политики безопасности, непрерывность и цикличность развития политики безопасности. Процесс разработки политики безопасности, организационные аспекты (постановка задачи, мотивация, обеспечение и контроль) процесса разработки. Инструментальные системы разработки и управления политиками безопасности
	6	2	**Практические правила управления информационной безопасностью.** Организационные вопросы безопасности. Классификация информации. Вопросы безопасности, связанные с персоналом. Физическая защита и защита от воздействий окружающей среды. Управление передачей данных и операционной деятельностью. Контроль доступа. Разработка и обслуживание систем. Управление непрерывностью бизнеса. Соответствие требованиям.

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
	7	2	**Аудит информационной безопасности.** Понятие аудита ИБ. Цели аудита. Объекты аудита ИБ. Виды аудита ИБ. Внешний аудит. Внутренний аудит. Методы аудита. Принципы проведения аудита. Структура отчёта о результатах аудита ИБ.
2	8	2	**Система комплексной защиты информации организации.** Цели и задачи комплексной защиты информации организации. Система комплексной защиты информации организации (СКЗИ). Порядок создания и ввода в эксплуатацию СКЗИ.
	9	2	**Предпроектное специальное обследование объектов информатизации** Определение перечня информации (сведений), подлежащих защите. Классификация сведений. Определение (выявление) актуальных угроз безопасности информации, связанных с утечкой информации по техническим каналам, НСД к защищаемой информации и с несанкционированным воздействием на информацию. Разработка модели угроз безопасности информации.
	10	2	**Техническое задание на создание системы комплексной защиты информации.** Подготовка исходных данных для формирования требований по защите информации (ЗИ): определения состава основных и вспомогательных технических средств и систем объекта информатизации; определение порядка обработки информации в автоматизированной системе (АС); оценка степени участия персонала в обработке (обсуждении, передаче, хранении) защищаемой информации; определение требуемого класса (уровня) защищенности АС от НСД; определение требований по защите объекта информатизации от утечки информации по техническим каналам. Обоснование рационального состава СКЗИ: выбор (обоснование) целесообразных способов и средств ЗИ от НСД, обоснование рационального состава системы защиты АС от НСД; выбор (обоснование) целесообразных способов и средств ЗИ от утечки по техническим каналам, обоснование рационального состава системы защиты объекта информатизации от утечки информации по техническим каналам; обоснование рационального состава системы физической защиты объекта информатизации; определение состав, содержания и сроков проведения работ по этапам разработки и внедрения СКЗИ; оценка возможности создания СКЗИ, исходя из ресурсных ограничений. Состав и содержание технического задания на создание СКЗИ. Порядок согласования и утверждения технического задания.
	11	2	**Проектирование системы комплексной защиты информации.** Порядок разработки (проектирования) СКЗИ. Стадия создания СКЗИ (эскизный проект; технический проект; рабочая документация). Работы, выполняемые при проектировании: разработка проектных решений по СКЗИ; разработка документации на СКЗИ; тестирование системы СКЗИ.

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
			Состав и содержание технического проекта СКЗИ. Порядок согласования и утверждения технического проекта.
	12	2	**Ввод системы комплексной защиты информации в эксплуатацию.** Внедрение системы СКЗИ: установка и настройка СКЗИ; разработка организационно-распорядительных документов, определяющих мероприятия по ЗИ в ходе эксплуатации СКЗИ; предварительные испытания СКЗИ; опытная эксплуатация и доработка СКЗИ; приемочные испытания СКЗИ. Аттестация объекта информатизации по требованиям безопасности информации.
	13	2	**Организация аттестации объектов информатизации требованиям по безопасности информации.** Порядок организации аттестации объектов информатизации требованиям по безопасности информации. Программа и методика аттестационных испытаний. Порядок проведения аттестационных испытаний. Заключение по результатам аттестационных испытаний. Аттестат соответствия.
	14	2	**Организации управления системой комплексной защиты информации.** Служба защиты информации организации: назначение, функциональная и организационная структуры, цели и задачи функционирования. Особенности деятельности службы защиты информации при управлении системой комплексной защиты информации в условиях чрезвычайных ситуаций.
	15	2	**Организация и обеспечение режима секретности (конфиденциальности) организации** Цели и задачи обеспечение режима секретности (конфиденциальности) организации. Организация пропускного режима в организации. Организация режима секретности (конфиденциальности) в организации. Порядок допуска должностных лиц к конфиденциальным документам.
	16	2	**Организация контроля состояния защиты информации на предприятии.** Определение контроля состояния защиты информации на предприятии. Основные требования к контролю. Виды, методы и средства контроля, их классификации и краткая характеристика. Порядок инициирования контрольных мероприятий, разработка программы и графика контрольных мероприятий, показатели и критерии контроля, организация реагирования на результаты контроля состояния защиты информации на предприятии.

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
1	1	4	**Семинар. Стандарты в области информационной безопасности** Классификация, структура и основное содержание основных международных и национальных стандартов в области информационной безопасности. Особенности применения международных и национальных стандартов в области ИБ в коммерческих и государственных структурах РФ. Корпоративные стандарты в области ИБ. Их назначение, структура и основное содержание. Особенности применения корпоративных стандартов в области ИБ в РФ.
	2	4	**Групповое упражнение.** Разработка проекта «Концепции информационной безопасности» организации **(**на примере коммерческой организации).
	3	4	**Групповое упражнение**. Разработка «Модели угроз безопасности информации» и «Модели нарушителя» **(**на примере автоматизированной системы обработки конфиденциальной информации).
	4	4	**Семинар. Политика информационной безопасности.** Практические правила управления информационной безопасностью.
2	5	4	**Групповое упражнение.** Предпроектное специальное обследование объекта информатизации **(**на примере автоматизированной системы обработки конфиденциальной информации).
	6	4	**Групповое упражнение.** Разработка технического задания на создание системы комплексной защиты объекта информатизации (на примере автоматизированной системы обработки конфиденциальной информации).
	7	4	**Групповое упражнение.** Разработка технического паспорта на объект информатизации (на примере автоматизированной системы обработки конфиденциальной информации).
	8	4	**Групповое упражнение.** Разработка организационно распорядительных по защите автоматизированной системы от НСД: Акт классификации автоматизированной системы (АС). Описание технологического процесса обработки информации в АС. Перечень защищаемых информационных ресурсов АС. Перечни объектов и субъектов доступа. Описание реализованных правил разграничения доступа. Инструкция администратора категорированной АС по обеспечению безопасности информации. Инструкция пользователя категорированной АС по обеспечению информационной безопасности.

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

Не предусмотрены

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	4	**Подготовка к семинару № 1:** Изучение материалов лекции №2 и 3. Изучение методических рекомендаций по подготовке и проведению семинара № 1 и рекомендованной литературы.
	4	**Подготовка к групповому упражнению №1:** Изучение материалов лекции №4. Изучение методических рекомендаций по подготовке и проведению ГУ № 1 и рекомендованной литературы.
	4	**Подготовка к групповому упражнению №2:** Изучение материалов лекции №5 и 6. Изучение методических рекомендаций по подготовке и проведению ГУ № 2 и рекомендованной литературы.
	4	**Подготовка к семинару № 2:** Изучение материалов лекции №5-7. Изучение методических рекомендаций по подготовке и проведению семинара № 2 и рекомендованной литературы.
	2	**Подготовка к компьютерному тесту КТ-1.** Изучение материалов лекций 1-7 и рекомендованной литературы.
2	4	**Подготовка к групповому упражнению №3:** Изучение материалов лекции №8 и 9. Изучение методических рекомендаций по подготовке и проведению ГУ № 3 и рекомендованной литературы.
	4	**Подготовка к групповому упражнению №4:** Изучение материалов лекции №8 и 109. Изучение методических рекомендаций по подготовке и проведению ГУ № 4
	4	**Подготовка к групповому упражнению №5:** Изучение материалов лекции №8-10. Изучение методических рекомендаций по подготовке и проведению ГУ № 5 и рекомендованной литературы.
	4	**Подготовка к групповому упражнению №6:** Изучение материалов лекции №11. Изучение методических рекомендаций по подготовке и проведению ГУ № 6 и рекомендованной литературы.
	2	**Подготовка к компьютерному тесту КТ-2.** Изучение материалов лекций 8-16 и рекомендованной литературы.
	28	**Выполнение курсового проекта:** «Разработка проекта технического задание на создание системы защиты информации объекта информатизации»

4.5. Примерная тематика курсовых работ (проектов)

Тема курсовой работы (КР) «Разработка проекта технического задания на создание системы защиты информации объекта информатизации».

Исследуемые объекты (по выбору студента):

объект информатизации на базе одной из аудиторий в корпусе №3 МИЭТ, окна которой не выходят во внутренний двор МИЭТ, в которой установлено автоматизированное рабочее место для обработки конфиденциальной информации на базе ПЭВМ и помещение выбранной аудитории, предназначенное для ведения конфиденциальных переговоров.

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. Основы управления информационной безопасностью:

Тексты лекций № 1 – 6. ОРИОКС// URL: http://orioks.miet.ru/

Методические рекомендации студентам по подготовке и проведению семинарских занятий № 1 – 2. ОРИОКС// URL: http://orioks.miet.ru/

Методические рекомендации студентам по подготовке и проведению групповых упражнений № 1 – 2. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Организация защиты информации в организации:

Тексты лекций № 7 – 12. ОРИОКС// URL: http://orioks.miet.ru/

Методические рекомендации студентам по подготовке и проведению групповых упражнений № 3 – 6. ОРИОКС// URL: http://orioks.miet.ru/

Методические рекомендации студентам по подготовке и написанию курсовой работы по дисциплине ОРИОКС// URL: http://orioks.miet.ru/.

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. 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 : Текст : непосредственный.

2. 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.

3. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. - М. : Юрайт, 2018. - 325 с. - (Бакалавр и магистр. Академический курс). - URL: https://urait.ru/bcode/413158 (дата обращения: 16.03.2021). - ISBN 978-5-534-03600-8.

4. Новиков В.К.Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. пособие. Ч. 1 :Правовое обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 184 с. - Имеется электронная версия изда-

ния. - ISBN 978-5-7256-0733-8.

5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. пособие. Ч. 2 Организационное обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 172 с. - ISBN 978-5-7256-0738-3.

6. Воеводин, В. А. Правовые основы аудита информационной безопасности: учебное пособие / В. А. Воеводин, П. Л. Пилюгин; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - Москва : МИЭТ, 2021. - 180 с. - ISBN 978-5-7256-0961-5 .

7. 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 : - Текст : непосредственный.

8. Программно-аппаратные средства защиты информации : учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5. - Текст : непосредственный.

9. 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: 15.03.2021). - ISBN 978-5-9912-0233-6.

10. 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 . - Текст : непосредственный.

11. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .

12. Хорев П.Б. Программно-аппаратная защита информации : Учеб. пособие / П.Б. Хорев. - М. : Форум, 2013. - 352 с. - (Высшее образование). - ISBN 978-5-91134-353-8 .

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

1. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;Information technology. Security techniques. Information security management systems. Requirements; Национальный стандарт РФ: Введ. 01.02.2008, (Переиздание январь 2019) М.: Стандартинформ, 2019- 31 л. -Текст: непосредственный.

2. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной без-

опасности Information technology. Security techniques. Code of practice for information security management ;Национальный стандарт РФ: Введ. 01.01.2014,-М.: Стандартинформ, 2014- 104 л. -Текст: непосредственный.

3. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» Information technology. Security techniques.Part 1. Concepts and models for information and communications technology security management;. Национальный стандарт РФ: Введ. 01.06.2007,-М.: Стандартинформ, 2007- 22 л. -Текст: непосредственный.

4. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Information technology. Security techniques. Information security risk management, Национальный стандарт РФ: Введ. 01.12.2011,-М.: Стандартинформ, 2011- 47 л. -Текст: непосредственный.

5. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети» Information technology. Security techniques. Part 5. Management guidance on network security; Национальный стандарт РФ: Введ. 01.06.2007, (Переиздание январь 2019) -М. Стандартинформ, 2019- 22 л. -Текст: непосредственный.

6. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» Information technology. Security techniques. Information security incident management, Национальный стандарт РФ: Введ. 01.07.2008 , (Переиздание апрель 2020), М.: Стандартинформ, 2020 - 46 л. -Текст: непосредственный.

7. ISO/IEC 27035-1 Информационные технологии. Методы безопасности. Управление инцидентами информационной безопасности - Часть 1: Принципы управления инцидентами; Information technology - Security techniques - Information security incident management- Part 1: Principles of incident management, Международный стандарт, ISO/IEC 2016 -28 л., -Текст: непосредственный.

8. ISO/IEC 27035-2 Информационные технологии. Методы безопасности. Управление инцидентами информационной безопасности - Часть 2. Руководство по планированию и подготовке к реагированию на инциденты; Information technology - Security techniques- Information security incident management- Part 2: Guidelines to plan and prepare for incident response; Международный стандарт, ISO/IEC 2016 - 64 л., -Текст: непосредственный.

9. Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации, Гостехкомиссия России, 2002, дсп.

10. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации, Гостехкомиссия России, 2002, дсп.

11. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2002, дсп.

12. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных техниче-

ских средствах и системах», Гостехкомиссия России, Москва, 2002, дсп.

13. 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.-8 л. - Текст: непосредственный.

14. 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.

15. 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.

16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Одобрены решением коллегии Гостехкомиссии России от 2 марта 2001 г. № 7.2, дсп.

17. 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 : [сайт]. – URL: https://docs.cntd.ru/document/901990051. - (дата обращения 15.03.2021)

Периодические издания

1. ЗАЩИТА ИНФОРМАЦИИ. INSIDE : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный : непосредственный.

2. 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.

3. 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. - Текст : электронный.

4. 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: 15.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ 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.

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).

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).

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
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 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. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL (Из реестра МИЭТ п.18) – 28 шт. 3. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 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:	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL 3. Корпоративная информационно - технологическая платформа ОРИОКС

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-5. ОУИБ. «Способен применять нормативные правовые акты, нормативные и методические документы при организации управления информационной безопасностью на объектах информатизации»

ФОС по подкомпетенции ОПК-6.ОУИБ. «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»

ФОС по компетенции ОПК-10. «Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты».

ФОС по подкомпетенции ОПК-12.ОУИБ. «Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации»

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

В целях практической подготовки в дисциплине предусмотрены практические занятия (семинары и групповые упражнения и выполнение курсового проекта.

11.1. Методические указания студентам по подготовке к семинарам

Семинар - развернутая беседа с обсуждением доклада. Проводится на основе заранее разработанного плана, по вопросам которого готовится вся учебная группа. Основными компонентами такого занятия являются: вступительное слово преподавателя, доклады обучаемых, вопросы докладчикам, выступления студентов по докладу и обсуждаемым вопросам, заключение преподавателя.

Развернутая беседа позволяет вовлечь в обсуждение проблем наибольшее число обучаемых. Главная задача преподавателя при проведении такого семинарского занятия состоит

в использовании всех средств активизации: постановки хорошо продуманных, четко сформулированных дополнительных вопросов, умелой концентрации внимания на наиболее важных проблемах, умения обобщать и систематизировать высказываемые в выступлениях идеи, сопоставлять различные точки зрения, создавать обстановку свободного обмена мнениями. Данная форма семинара способствует выработке у обучаемых коммуникативных навыков.

Как правило, темы докладов разрабатываются преподавателем заранее и включаются в планы семинаров. Доклад носит характер краткого (10-15 мин.) аргументированного изложения одной из центральных проблем семинарского занятия с использованием презентации.

В ходе семинаров заслушиваются выступления по вопросам семинара, также доклады по рефератам, темы которых соответствующих вопросам, рассматриваемым на семинаре.

11.2. Методические указания студентам по подготовке к групповым упражнениям

Выполнение студентами групповых упражнений (ГУ) 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 целью 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 исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, оформлять результаты).

Групповое упражнение, как вид учебного занятия проводиться в мультимедийных аудиториях. Продолжительность - не менее двух академических часов.

По каждому ГУ разработаны и утверждены методические указания по их проведению.

Групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория), порядок выполнения работы, контрольные вопросы, учебная и специальная литература.

Формы организации студентов на ГУ: индивидуальная, при которой каждый студент выполняет индивидуальное задание.

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

Методические рекомендации по выполнению ГУ работ включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на ГУ;

- наименование темы ГУ;
- цель 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 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 ГУ студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ГУ;
- ознакомиться с методическими рекомендации по выполнению 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 ГУ;
- подготовить отчеты для заполнения.

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

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

При защите отчета о 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, после чего отчитаться в проделанной работе перед преподавателем.

11.3. Методические указания студентам по подготовке курсовой работы

Тема курсовой работы (КР) «Разработка проекта технического задание на создание системы защиты информации объекта информатизации».

Целевая установка КР: На основе анализа угроз безопасности информации объекта информатизации, способов и средств защиты информации провести аналитическое обоснование необходимости создания системы защиты объекта информатизации (ОИ) и разработать проект технического задания на ее создание.

Задачи выполнения КР:

обучение студентов самостоятельному применению полученных знаний для решения конкретных практических задач по обоснованию необходимости разработки системы защиты информации ОИ и разработке технического задания на ее создание;

развитие навыков подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по организации и проведению работ по разработке системы защиты ОИ;

получение навыков предпроектного специального обследования ОИ;

получение навыков проведения аналитического обоснования необходимости создания системы защиты ОИ.

получение навыков разработки технического задания на создание системы защиты ОИ.

Исследуемые объекты (по выбору студента):

объект информатизации на базе одной из аудиторий в корпусе №3 МИЭТ, окна которой не выходят во внутренний двор МИЭТ, в которой установлено автоматизированное рабочее место для обработки конфиденциальной информации на базе ПЭВМ и помещение выбранной аудитории, предназначенное для ведения конфиденциальных переговоров.

Основные вопросы, подлежащие разработке при выполнении курсовой работы:

1. В рамках анализа объекта информатизации как объекта защиты информации провести:

Анализ назначения защищаемого объекта информатизации (далее по тексту – защищаемого объекта);

Анализ технических средств, входящих в состав автоматизированного рабочего места для обработки конфиденциальной информации (далее по тексту – ОТСС), установленных на объекте информатизации и непосредственно участвующие в обработке конфиденциальной информации, составление их перечня;

Анализ информации, обрабатываемой в АС. Разработка перечня сведений ограниченного доступа, обрабатываемого в АС;

Анализ общесистемных и специальных программных средств, используемых для обработки информации;

Анализ подключений АС к сетям общего пользования;

Разработать перечень лиц, имеющих право доступа к АС и обрабатываемой в ней информации;

Провести классификацию АС;

Анализ вспомогательных технических средств и систем (ВТСС) установленные на объекте информатизации, составление их перечня;

Разработать схему расположения мебели, ОТСС и ВТСС в защищаемом помещении;

Анализ местоположения защищаемого объекта на местности и определение границы его контролируемой зоны;

Анализ системы электропитания и заземления защищаемого объекта;

Анализ месторасположения трансформаторной подстанции и заземлителя относительно границы контролируемой зоны объекта;

Анализ инженерных коммуникаций, посторонних проводников и соединительные линии ВТСС, выходящих за пределы контролируемой зоны объекта;

Провести описание защищаемого помещения (входа в помещение, пола, потолка, стен, окон, системы вентиляции и кондиционирования);

Определить наличия физической охраны здания, в котором расположено предприятие (учреждение);

Определить наличие системы охранной сигнализации, охранного телевидения, системы контроля и управления доступом в служебные и технические помещения предприятия (учреждения);

Описать порядок доступа сотрудников и посторонних лиц на предприятие (в учреждение);

Описать порядок доступа сотрудников предприятия (учреждение), а также посторонних лиц на объект информатизации в служебное и неслужебное время;

Описать и провести анализ организационных мероприятий по технической защите информации, реализуемых в учреждении;

Провести анализ технических средств защиты объекта информатизации от утечки информации по техническим каналам;

Провести анализ технических средств защиты выделенного помещения от утечки речевой информации по техническим каналам.

2. В рамках анализа угроз безопасности информации объекта информатизации провести:

Анализ возможностей заинтересованных субъектов по перехвату информации, обрабатываемой ПЭВМ, по каналу утечки информации, возникающему за счет побочных электромагнитных излучений (ПЭМИ) ПЭВМ и каналам утечки информации, возникающим за счет наводок ПЭМИ ПЭВМ на токопроводящие коммуникации, линии электропитания и цепи заземления;

Анализ возможностей непреднамеренного прослушивания конфиденциальных разговоров, ведущихся в выделенном помещении, посторонними лицами;

Анализ возможностей заинтересованных субъектов по перехвату конфиденциальных разговоров, ведущихся в выделенном помещении:

с использованием лазерных акустических систем разведки (ЛАСР) и направленных микрофонов;

электронных стетоскопов и радиостетоскопов;

аппаратуры «высокочастотного навязывания» и средств, подключаемых к соединительным линиям ВТСС;

электронных устройств перехвата речевой информации, возможно внедренных в выделенное помещение;

Разработать перечень потенциальных технических каналов утечки информации, обрабатываемой ОСТТ с указанием возможных средства перехвата информации (стационарных, мобильных и портативных) и мест их возможной установки;

Разработать перечень потенциальных технических каналов утечки речевой информации из выделенных помещений (стационарных, мобильных и портативных) и мест их возможной установки;

Разработать модель нарушителя (злоумышленника);

Провести анализ угроз безопасности информации, обрабатываемой на АС;

Разработать модель угроз информации, обрабатываемой на АС.

3. На основе анализа угроз безопасности информации:

а) *Обосновать требования и рациональный состав системы защиты информации от утечки по техническим каналам:*

обосновать требования, предъявляемые к системе защиты объекта информатизации от утечки информации по техническим каналам;

обосновать требования, предъявляемые к техническим средствам защиты объекта информатизации от утечки информации по техническим каналам;

провести анализ пассивных и активных технических средств защиты информации, обрабатываемой ОТСС, по каналу утечки информации, возникающему за счет побочных электромагнитных излучений ОТСС (для сравнения характеристики анализируемых средств защиты сводятся в таблицы);

провести анализ пассивных и активных технических средств защиты информации, обрабатываемой ОТСС, по каналу утечки информации, возникающему за счет наводок побочных электромагнитных излучений ОТСС на токопроводящие коммуникации, линии электропитания и цепи заземления (для сравнения характеристики анализируемых средств защиты сводятся в таблицы);

провести сравнительную оценку (по показателю эффективность – стоимость) технических средств защиты информации от утечки по техническим каналам, предполагаемых для установки на объекте информатизации;

определить рациональный состав системы защиты объекта информатизации от утечки информации по техническим каналам, составить перечень предполагаемых к использованию технических средств защиты (в перечне указать для закрытия каких технических каналов информации предполагается использовать техническое средство защиты);

обосновать требования, предъявляемые к системе защиты выделенного помещения от утечки речевой информации по техническим каналам;

обосновать требования, предъявляемые к техническим средствам защиты выделенного помещения от утечки речевой информации по техническим каналам;

провести анализ систем виброакустической маскировки (для сравнения характеристики анализируемых систем свести в таблицы);

провести анализ специальной аппаратуры для ведения конфиденциальных переговоров;

провести анализ способов и средств защиты ВТСС от утечки информации по акустоэлектрическим каналам (для сравнения характеристики анализируемых средств защиты свести в таблицы);

провести анализ способов и средств подавления средств перехвата речевой информации (подавителей: диктофонов, радиозакладок, сетевых закладок, сотовой связи, средств беспроводного доступа и т.п.) (для сравнения характеристики анализируемых средств защиты свести в таблицы);

провести сравнительную оценку (по показателю эффективность – стоимость) технических средств защиты информации от утечки речевой по техническим каналам, предполагаемых для установки выделенном помещении;

определить рациональный состав системы защиты выделенного помещения от утечки речевой информации по техническим каналам, составить перечень предполагаемых к использованию технических средств защиты (в перечне указать для закрытия каких технических каналов информации предполагается использовать техническое средство защиты).

б) Обосновать требования и рациональный состав системы защиты информации от несанкционированного доступа:

обосновать требования, предъявляемые к системе защиты АС от несанкционированного доступа к информации;

разработать организационные мероприятия по защите АС от несанкционированного доступа к информации;

провести сравнительный анализ сертифицированных программных и программно-аппаратных средств защиты АС от несанкционированного доступа к информации, удовлетворяющих предъявляемым требованиям;

провести сравнительный анализ сертифицированных средств антивирусной защиты;

определяется рациональный состав системы защиты АС от несанкционированного доступа к информации (СЗИ НСД);

разработать перечень организационно-распорядительных документов, которые должны быть разработаны на объекте информатизации;

определить этапы и ориентировочные сроки разработки и внедрения СЗИ НСД.

в) *Обосновать требования и рациональный состав системы физической защиты объекта информатизации:*

обосновать требования, предъявляемые к системе физической защиты объекта информатизации;

провести сравнительный анализ средств контроля и управления доступом на объект информатизации, удовлетворяющих предъявляемым требованиям;

провести сравнительный анализ средств охранной и пожарной сигнализации объекта информатизации, удовлетворяющих предъявляемым требованиям;

провести сравнительный анализ средств охранного телевидения объекта информатизации, удовлетворяющих предъявляемым требованиям;

определить рациональный состав системы физической защиты объекта информатизации;

определить этапы и ориентировочные сроки разработки и внедрения системе физической защиты объекта информатизации.

4. На основе проведенных исследований разработать проект технического задания на создание технического задания на создание системы защиты ОИ.

Курсовой проект 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 курсового проекта должна отвечать традиционным требованиям, предъявляемым к научным работам и включать следующие части (структурные элементы):

Титульный лист.

Задание на КР.

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 КР с основными сведениями о выполненных разработках и полученных результатах.

Реферат имеет следующую структуру:

− перечень количественных сведений о КР;

− перечень ключевых слов;

− текст реферата.

Перечень количественных сведений о КР 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;

− о цели создания системы защиты информации;

− об использованных методах и средствах, использованных при исследовании объекта информатизации;

− о результатах исследования объекта информатизации.

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 КР, 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 исследования объекта информатизации;

− 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:

- анализ объекта информатизации как объекта защиты информации,

- анализ угроз безопасности информации объекта информатизации,

- обоснование требований и рационального состава системы защиты информации от утечки по техническим каналам,

- обоснование требований и рационального состава системы защиты информации от несанкционированного доступа,

- обоснование требований и рационального состава системы физической защиты объекта информатизации,

- проект технического задания на создание системы защиты информации объекта информатизации согласно ГОСТа 34.602-89 «Техническое задание на создание автоматизиро-

ванной системы» и ГОСТ Р 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении».

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 КР, 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 Р 7.0.100-2018. «Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления" (утв. и введен в действие Приказом Росстандарта от 03.12.2018 N 1050-ст)».

Приложения. В приложения выносится проект технического задания на создание автоматизированной системы обработки информации, схемы измерений, планы и план-схемы объекта информатизации, схемы электропитания, заземления объекта, схемы инженерных коммуникаций, линий связи и т.д.

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.

Курсовые проекты размещаются в разделе «Портфолио» электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/.

11.4. Система контроля и оценивания

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

Под накопительно-бальной системой 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 мероприятий текущего контроля (сдача компьютерных тестов, защита отчетов по групповым упражнениям, доклады на семинарских занятиях, защита курсовой работы), 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
2	Семинар № 1	4	2
4	Групповое упражнение № 1	8	4
6	Групповое упражнение № 2	8	4
8	Семинар № 2	4	2
8	Компьютерный тест (КТ-1)	4	2
10	Групповое упражнение № 3	8	4
12	Групповое упражнение № 4	8	4
14	Групповое упражнение № 5	8	4
16	Групповое упражнение № 6	8	4
16	Компьютерный тест (КТ-2)	4	2
16	Посещаемость, активность	4	2
	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

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
10	Контроль № 1	10	5
12	Контроль № 2	10	5
14	Контроль № 3	10	5
16	Итоговый просмотр (оценка качества курсового проекта)	40	20
	Итого за текущий контроль	***70***	***35***
17	***Итоговый контроль*** *(защита курсового про-*	***30***	***15***

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
	екта)		
	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

Доцент кафедры «Информационная безопасность»
кандидат технических наук_____ Р.Я. Панцыр

Рабочая программа дисциплины «Основы управления информационной безопасностью» по направлению подготовки 10.03.01 «Информационная безопасность», направленности (профилю) «Техническая защита информации» 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 /