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
«Правовые основы аудита информационной безопасности»

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**:**

Компетенция ПК-3 «Способен проводить аудит информационной безопасности» сформулирована на основе проекта новой редакции профессионального стандарта 064.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).

Обобщенная трудовая функция D/7. Аудит информационной безопасности автоматизированной системы.

Трудовая функция D/01.7. Подготовка к проведению аудита информационной безопасности автоматизированной системы.

Трудовая функция D/02.7. Проведение аудита информационной безопасности автоматизированной системы.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-3. Способен проводить аудит информационной безопасности	ПК-3. ПОАИБ. Способен использовать нормативные правовые акты, национальные стандарты при проведении аудита информационной безопасности.	**Знания** основные нормативные правовые акты в области обеспечения информационной безопасности; основные международные и национальные стандарты в области информационной безопасности; основные нормативные и методические документы ФСТЭК России и ФСБ России в области информационной безопасности и защиты информации; правовые основа аудита информационной безопасности и аттестации объектов информатизации; основные международные и национальные стандарты в области аудита информационной безопасности; основные нормативные и методические документы в области аудита информационной безопасности и аттестации объектов информатизации; ответственность за преступления в сфере информационной безопасности.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		Умения: использовать нормативные правовые акты, национальные стандарты при проведении аудита информационной безопасности. **Опыт практической деятельности:** подготовки обзоров и докладов в области правового обеспечения аудита информационной безопасности.

В результате изучения дисциплины студент должен:

Знать:

- основные нормативные правовые акты в области обеспечения информационной безопасности;
- основные международные и национальные стандарты в области информационной безопасности;
- основные нормативные и методические документы ФСТЭК России и ФСБ России в области информационной безопасности и защиты информации;
- правовые основа аудита информационной безопасности и аттестации объектов информатизации;
- основные международные и национальные стандарты в области аудита информационной безопасности;
- основные нормативные и методические документы в области аудита информационной безопасности и аттестации объектов информатизации;
- ответственность за преступления в сфере информационной безопасности.

Уметь:

- использовать нормативные правовые акты, национальные стандарты при проведении аудита информационной безопасности.

Иметь практический опыт:

- подготовки обзоров и докладов в области правового обеспечения аудита информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Правовые основы аудита информационной безопасности» входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 1-м курсе в 1-м семестре и является дисциплиной по выбору.

Изучение дисциплины базируется на знаниях и умениях, полученных при освоении основной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность при изучении следующих дисциплин: «Правоведение», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Знания и умения, полученные в результате изучения дисциплины, используются в дисциплинах «Организация аудита информационной безопасности», «Аудит информационной безопасности автоматизированных систем (деловая игра)», 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	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1	1	5	180	80	32	-	32	16	64	Экз. (36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы					Самостоятельная работа, часы	Вид промежуточной аттестации
	ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1. Правовые основы информационной безопасности.	40	16	-	16	8	32	Компьютерный тест КТ-1.
2. Правовые основы аудита информационной безопасности.	40	16	-	16	8	32	Компьютерный тест КТ-2.

4.1. Лекционные занятия

Номер модуля дисциплины	**Номер лекции**	**Объем занятий, часы**	**Краткое содержание**
1	1.	4	**Правовые основы обеспечения информационной безопасности.** Введение в учебную дисциплину. Основы правового и нормативного регулирования. Правовые нормативные основы обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности (ИБ).
	2.	4	**Правовое, нормативное и методическое обеспечения информационной безопасности** Иерархия нормативных правовых актов в области ИБ. Федеральные законы и Указы Президента Российской Федерации в области ИБ. Постановления Правительства Российской Федерации в области ИБ. Международные и национальные стандарты в области ИБ.
	3.	4	**Система правового и нормативного обеспечения защиты информации в Российской Федерации** Полномочия и права государственных органов в области ЗИ. Система правовых актов ЗИ. Система стандартов по ЗИ.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			Приказы, нормативные и методические документы (НМД) ФСБ России, ФСТЭК России в области ЗИ.
	4.	4	**Правовые основы порядок организации и осуществления государственного и муниципального контроля** Правовые основы государственного контроля (надзора) в области защиты информации. Виды проверок, содержание, сроки и продолжительность их проведения. Порядок организации и проведения проверки. Оформление результатов проверки. Ответственность за нарушения законодательства в области государственного контроля (надзора).
2	5.	4	**Правовое, нормативное и методическое обеспечение аудита информационной безопасности** Ведение в предметную область. Общая характеристика состояния аудиторской деятельности в области информационной безопасности. Основные виды и способы аудита информационной безопасности. Основные принципы аудита информационной безопасности. Критерии аудита информационной безопасности. Организационно-методологические основы проведения аудита информационной безопасности. Инструментальное обеспечение аудита информационной безопасности. Требования к кадровому обеспечению аудиторской деятельности в области информационной безопасности.
	6.	4	**Правовое, нормативное и методическое обеспечение внутреннего аудита информационной безопасности** Концептуальные основания внутреннего аудита ИБ. Место внутреннего аудита ИБ в управленческой иерархии предприятия. Регламентация деятельности внутреннего аудита. Постановка задачи внутреннего аудита.
	7.	4	**Правовое, нормативное и методическое обеспечение внешнего аудита информационной безопасности** Внешний аудит ИБ как систематический, независимый и документированный процесс получения свидетельства деятельности организации по ОИБ; Принципы проведения внешнего аудита ИБ; Управление программой внешнего аудита ИБ; Этапы проведения внешнего аудита ИБ; Компетентность аудиторов ИБ; Взаимоотношения представителей аудиторской группы и проверяемых организаций; Требования стандартов ISO/IEC27001:2005 и ГОСТ Р ИСО/МЭК 27001-2006, ISO/IEC27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011, ISO/IEC27006:2011 и ГОСТ Р ИСО/МЭК 27006-2008, ISO/IEC27007:2011 и ISO/IEC27008:2011, ISO/IEC19011:2002 и ГОСТ Р ИСО/МЭК 19011-2003 по проведению внешнего аудита
	8.	4	**Правовое и нормативное обеспечение аудита информационных систем различного назначения** Федеральный закон "О безопасности критической информацион-

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			ной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ. Структура системы подзаконных актов. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» ФЗ № 152 «О персональных данных». Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Особенности проведения аудита информационной безопасности ИСПДн, ГИС, АСУ ТП.

4.2. Практические занятия

Номер модуля дисциплины	Номер ПЗ	Объем занятий, часы	Краткое содержание
1.	1.	4	**Практическое занятие (семинар). Правовое, нормативное и методическое обеспечение информационной безопасности** Обзор федеральных законов и указов Президента, Постановлений Правительства РФ в области ИБ.
	2.	4	**Практическое занятие (семинар). Международные и отечественные стандарты в области информационной безопасности** Международные стандарты в области ИБ. Национальные стандарты в области ИБ и ЗИ.
	3.	4	**Практическое занятие (семинар). Система обеспечения информационной безопасности Российской Федерации. Полно-**

Номер модуля дисциплины	Номер ПЗ	Объем занятий, часы	Краткое содержание
			мочия ФСБ и Роскомнадзора России в области информационной безопасности Структура системы обеспечения информационной безопасности Российской Федерации. Структура, полномочия ФСБ. Структура и полномочия Роскомнадзора. Задачи ФСБ в области обеспечения защиты информации. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Организация разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности. Требования к средствам электронной подписи. Требования к средствам удостоверяющего центра. Требования по защите информации, содержащейся в информационных системах общего пользования. О российском государственном сегменте информационно-телекоммуникационной сети "Интернет".
	4.	4	**Практическое занятие (семинар). Система обеспечения информационной безопасности Российской Федерации. Полномочия ФСТЭК в области информационной безопасности** Структура и полномочия ФСТЭК. Правовые средства ФСТЭК для обеспечения защиты информации. Требования к обеспечению защиты информации, не содержащей государственную тайну, содержащейся в государственных информационных системах (ГИС). Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Требования о защите информации, содержащихся в информационных системах общего пользования. Требования и методы по обезличиванию персональных данных. Методические рекомендации по обезличиванию персональных данных. Конвенция об обеспечении международной информационной безопасности (концепция). Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.
2	5.	4	**Практическое занятие (семинар). Правовое, нормативное и методическое обеспечение аудита информационной безопас-**

Номер модуля дисциплины	Номер ПЗ	Объем занятий, часы	Краткое содержание
			ности Правовые основы внутреннего аудита информационной безопасности. Правовые основы внешнего аудита информационной безопасности организаций на соответствие требованиям международных и национальных стандартов в области ИБ.
	6.	4	**Практическое занятие (семинар). Правовое, нормативное и методическое обеспечение аттестации объектов информатизации** Сущность, предназначение, цели и задачи аттестации объектов информатизации. Основные нормативно-правовые документы, определяющие цели и задачи, порядок и условия проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации. Порядок проведения аттестации и контроля. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации. Требования к нормативным и методическим документам по аттестации объектов информатизации
	7.	4	**Практическое занятие (семинар). Правовое, нормативное и методическое обеспечение аудита информационных систем критической инфраструктуры** Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» Ответственность за нарушение требований действующего законодательства.
	8.	4	**Практическое занятие (семинар). Правовое, нормативное и методическое обеспечение аудита информационных систем персональных данных** Законодательство Российской Федерации в области защиты персональных данных. Требования ФЗ № 152 «О персональных данных». Принципы и условия обработки персональных данных. Конфиденциальность персональных данных. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных. Контроль и надзор за обработкой персональных данных. Аудита информа-

Номер модуля дисциплины	Номер ПЗ	Объем занятий, часы	Краткое содержание
			ционных систем персональных данных. Ответственность за нарушение требований действующего законодательства.

4.3. Лабораторные работы

(не предусмотрены)

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	4	**Подготовка к практическому занятию (семинару) № 1** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Изучение плана проведения семинара № 1. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 2** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Изучение плана проведения семинара № 2. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 3** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Изучение плана проведения семинара № 3. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 4** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы. Изучение плана проведения семинара № 4. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к компьютерному тесту КТ-1** Изучение материалов лекции №№ 1 - 4 и рекомендованной литературы.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
2	4	**Подготовка к практическому занятию (семинару) № 5** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы. Изучение плана проведения семинара № 5. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 6** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы. Изучение плана проведения семинара № 6. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 7** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы. Изучение плана проведения семинара № 7. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 8** Изучение материалов лекции №№ 5 -84 и рекомендованной литературы. Изучение плана проведения семинара № 8. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к компьютерному тесту КТ-2** Изучение материалов лекции №№ 5 - 8 и рекомендованной литературы.
1,2	24	**Подготовка реферата**

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 «Правовые основы информационной безопасности»:

Тексты лекций № 1 – 4. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения практических занятий (семинаров) № 1 – 4. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2 «Правовые основы аудита информационной безопасности»:

Тексты лекций № 5 – 8. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения практических занятий (семинаров) № 4 – 8. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

1. Воеводин, В. А. Аудит информационной безопасности автоматизированных систем учебное пособие / В. А. Воеводин, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0974-5 : - 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: 15.03.2021). - ISBN 978-5-534-03600-8. - Текст : электронный.
4. 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 - Текст : непосредственный.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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 .

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

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция).
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
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; Computers technique. Information protection against unauthorised access to information. General technical requirements: Национальный стандарт РФ: Введ. 01.01.1996: М.: Издательство стандартов, 1995 Стандар-

тинформ, 2006.- URL: https://docs.cntd.ru/document/9039120 (дата обращения 16.03.2021).- Текст: электронный.

15. ГОСТ Р 50922-2006 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 (дата обращения 16.03.2021).- 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: 10.03.2021)- 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.

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. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».- (с изменениями на 15 марта 2021 года) .-Текст: электронный// Техэксперт : [сайт]. URL: https://docs.cntd.ru/document/499084780 , (дата обращения: 16.03.2021)- Текст: электронный.

21. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».Текст: электронный// Техэксперт: [сайт]. -URL:https://docs.cntd.ru/document/499034326, (дата обращения: 16.03.2021)- Текст: электронный.

22. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».- Текст: электронный// Техэксперт : [сайт]. URL: https://docs.cntd.ru/document/499002630 , (дата обращения: 16.03.2021)- Текст: электронный.

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: 16.03.2021). - 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.
4. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 10.03.2021). - Текст: электронный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе 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 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 самостоя-	Компьютерная техника с	1. Неисключительное право

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
тельной работы обучающихся: Учебная аудитории № 3226	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.	на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информационно - технологическая платформа ОРИОКС

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ПК-3.ПОАИБ «Способен использовать нормативные правовые акты, национальные стандарты при проведении аудита 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

В целях практической подготовки в дисциплине предусмотрены практические занятия (семинары) и подготовка реферата.

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 рефератов

Реферат представляет собой отчет об изучении студентом конкретной задачи (вопроса).

Перечень возможных тем рефератов:

1. Правовое обеспечение информационной безопасности.
2. Государственная система правового регулирования в области ИБ личности, общества, государства и современных автоматизированных и телекоммуникационных систем.
3. Предназначение, структура и полномочия органов государственного управления в области обеспечения ИБ.
4. Нормативные правовые акты РФ в области обеспечения ИБ.
5. Международные и национальные стандарты в области ИБ
6. Приказы, нормативные и методические документы ФСБ Росси в области ИБ и ЗИ.
7. Приказы, нормативные и методические документы ФСТЭК России в области ИБ и ЗИ.
8. Правовые основы лицензирования в области защиты информации в РФ.
9. Порядок лицензирования деятельности в области ТЗИ.
10. Порядок лицензирования деятельности при использовании СТС.
11. Правовые основы государственного контроля и надзора в области защиты информации.
12. Правовое регулирование ИБ в сфере интеллектуальной собственности.

13. Правонарушения в сфере компьютерной информации и особенности расследования компьютерных преступлений.
14. Юридическая ответственность за нарушение правовых норм в области ИБ.
15. Проблемные вопросы правового регулирования в области информационной безопасности.

Модуль 2

16. Нормативное обеспечение проверки и оценки деятельности по обеспечению ИБ.
17. Правовое обеспечение процессов проверки системы обеспечения ИБ (мониторинг ИБ, самооценка ИБ, внутренний аудит ИБ).
18. Правовые основы организации и порядок проведения внутреннего аудита.
19. Правовое обеспечение проведения внешнего аудита ИБ организации.
20. Правовые основы взаимоотношения представителей аудиторской группы и проверяемых организаций.
21. Анализ нормативно-правовых документов, определяющих цели и задачи, порядок и условия проведения аттестации объектов информатизации.
22. Правовые основы государственного контроля и надзора и инспекционного контроля за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации.
23. Правовое обеспечение применения инструментальных средств аудита ИБ.
24. Документальное оформление оценки эффективности и результативности деятельности по обеспечению ИБ в организации.
25. Правовые основы расследования компьютерных преступлений и инцидентов в области ИБ
26. Международные и национальные стандарты в области аудита ИБ
27. Правовые основы аудита информационной безопасности организаций
28. Правовые основы аттестации объектов информатизации.
29. Правовые основы аудита информационных систем персональных данных.
30. Правовые основы аудита АСУ ТП КИИ.
31. Правовые основы аудита информационной безопасности организаций банковской системы Российской Федерации

Реферат должен состоять из следующих частей (структурных элементов):

Титульный лист является первым листом в реферате.

Перечень условных обозначений и сокращений. Принятые в реферате 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 реферата 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 развернутую оценку современного состояния решаемой задачи. Объем введения 1 − 3 страницы.

Основная часть. Основная часть включает два – три раздела.

Первый раздел носит обычно просветительский характер и посвящен описанию основных положений, методов, способов и подходов, используемых для решения поставленной задачи. В этот раздел включается только то, что необходимо в качестве исходной основы для понимания сути проведенных исследований, описанных в последующих разделах. Остальные разделы содержат конкретные результаты исследований.

Заключение должно содержать краткие выводы по результатам выполнений работы. Типовой объем заключения составляет 1-2 страницы.

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

Приложения. В приложения рекомендуется включать материалы, связанные с выполненной работой, которые по каким-либо причинам не могут быть включены в основную часть. 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.

Общий объем реферат составляет до 24 страниц (без приложений). Не следует объем делать более 30 страниц (с приложениями).

При изложении текста реферата следует руководствоваться ГОСТ 7.32-2017 «Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления».

Реферат оформляется в редакторе Word, шрифт Times New Roman размер – 12-14 интервал – полуторный (30 строк по 60 печатных знаков в каждой строке, считая пробелы). Размеры полей следующие: левое – 30 мм, правое — не менее 10 мм, верхнее - не менее 20 мм, нижнее — не менее 20 мм. Отступ красной строки 1,25 см.

Изложение реферата должно быть выдержано в строгом литературном стиле, принятом для научно-технических отчетов и научных публикаций. Не следует использовать жаргоны и вульгаризмы. Это относится как к авторскому тексту, так и к текстам, заимствованным из различных не рецензируемых и не проходящих корректуру электронных публикаций в Internet. Не следует в пределах реферата применять для одних и тех же понятий различные термины. Нежелательно также применение иностранных слов и терминов при наличии равнозначных общепринятых в данной области русскоязычных слов и терминов. При первом упоминании термина его синонимы, используемые в данной области, можно перечислить, а

затем пользоваться только одним из них. Следует использовать только общепринятые аббревиатуры, сокращения, условные обозначения, символы, единицы и термины.

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

11.3. 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, доклады на семинарских занятиях, доклады с рефератами), 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 – $R_{нор}$).

Примерные 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
3	Практическое занятие (семинар) № 1	6	3
3	Практическое занятие (семинар) № 2	6	3
6	Практическое занятие (семинар) № 3	6	3
7	Практическое занятие (семинар) № 4	6	3
8	Компьютерный тест КТ-1	4	2
9	Практическое занятие (семинар) № 5	6	3
10	Практическое занятие (семинар) № 6	6	3
11	Практическое занятие (семинар) № 7	6	3
12	Практическое занятие (семинар) № 8	6	3
14	Компьютерный тест КТ-2	4	2
16	Посещаемость, активность	4	2
17	Реферат	12	6
	Итого за текущий контроль	***72***	***36***
	Итоговый контроль	***28***	***14***
	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

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.

РАЗРАБОТЧИК
Доцент кафедры «Информационная безопасность»
Кандидат технических наук _____ В.А. Воеводин

Рабочая программа дисциплины «Правовые основы аудита информационной безопасности» 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 /