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 информационной безопасности»

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-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1. ОИБ. Способен оценивать роль информации и информационной безопасности в современном обществе	**Знания:** место и роль информационной безопасности в системе национальной безопасности Российской Федерации, в обеспечении защиты интересов личности, общества и государства; основные положения «Доктрины информационной безопасности Российской Федерации»; цели, задачи и направления защиты информации; основные нормативные правовые акты в области информационной безопасности и защиты информации. **Умения:** аргументировать социальную значимость своей будущей профессии и мотивацию к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства. **Опыт практической деятельности:** подготовки рефератов по вопросам информационной безопасности.

В результате изучения дисциплины студент должен:

Знать:

место и роль информационной безопасности в системе национальной безопасности Российской Федерации, в обеспечении защиты интересов личности, общества и государства;

основные положения «Доктрины информационной безопасности Российской Федерации»;

цели, задачи и направления защиты информации;

основные нормативные правовые акты в области информационной безопасности и защиты информации;

направления подготовки (специальности, профили подготовки) в области информационной безопасности;

основные требования федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация «бакалавр»).

Уметь:

аргументировать социальную значимость своей будущей профессии и мотивацию к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства.

Иметь опыт деятельности:

подготовки докладов и рефератов по вопросам информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

Дисциплина является первой, из профессиональных дисциплин в области информационной безопасности.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении следующих дисциплин: «История», «Философия», «Информатика».

Знания и умения, полученные в результате изучения дисциплины, используются во всех дисциплинах в области информационной безопасности.

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		
2	3	3	108	60	32	-	16	12	48	Зачет

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля (раздела)	Контактная работа, часы					Самостоятельная работа, часы	Формы текущего контроля
	Всего	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1. Угрозы безопасности информации, цели и задачи защиты информации	38	22	-	8	8	24	Защита реферата
2. Информационная безопасность Российской Федерации	22	10	-	8	4	24	Защита реферата

4.1. Лекционные занятия

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
1	1.	2	**Информация – как объект защиты.** Определение информации. Виды информации. Сведения, составляющие государственную тайну. Конфиденциальная информация. Безопасность информации (определение). Свойства безопасности информации: конфиденциальность, доступность, целостность.
	2.	2	**Классификация угроз безопасности информации.** Объекты защиты (объект информатизации, выделенное помещение, телекоммуникационная система). Классификация угроз безопасности информации. Угрозы конфиденциальности информации: разглашение, хищение носителей информации, утечка информации по техническим каналам, несанкционированный доступ к информации. Угрозы целостности и доступности информации Ответственность за реализацию угроз безопасности информации: ответственность за разглашение сведений ограниченного доступа, ответственность за хищение носителей информации, ответственность за перехват информации ТСР, ответственность за несанкционированный доступ к информации.
	3.	2	**Технические каналы утечки информации, обрабатываемой СВТ и АС.** Классификация технических каналов утечки информации, обрабатываемой СВТ и АС. Технические каналы утечки информации, возникающие за счет ПЭМИН. Специально создаваемые технические каналы утечки информации.
	4.	2	**Технические каналы утечки акустической речевой информации.**

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			Классификация технических каналов утечки акустической речевой информации. Прямые акустические каналы утечки информации. Акустовибрационные и акустооптические каналы утечки информации Акустоэлектрические и акустоэлектромагнитные каналы утечки информации
	5.	2	**Несанкционированный доступ к информации**. Угрозы несанкционированного доступа к информации. Способы несанкционированного доступа к информации. Уровни нарушителей правил доступа к информации. Угрозы целостности и доступности информации: неправомерное модифицирование (искажение, подмена), уничтожение информации, неправомерное блокирование доступа к информации).
	6.	2	**Основные направления и задачи защиты информации.** Защита информации - определение. Виды (направления) защиты информации (правовая защита информации, техническая защита информации, криптографическая защита информации, физическая защита объектов информатизации). Основные задачи защиты информации. Ответственность за незаконную деятельность по зашита информации и невыполнение требований по защите информации.
	7.	2	**Способы и средства защиты объектов информатизации от утечки информации по техническим каналам.** Классификация способов и средств защиты объектов информатизации от утечки информации по техническим каналам. Экранирование и заземление технических средств. Системы пространственного электромагнитного зашумления. Способы и средства защиты объектов информатизации от утечки информации по цепям электропитания и заземления.
	8.	2	**Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам** **Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.** Звуко- и виброизоляция выделенных помещений Системы и средства виброакустической маскировки. Средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам. Специальные технические средства подавления электронных устройств перехвата речевой информации.
	9.	2	**Способы и средства защиты информации от несанкционированного доступа.** Способы защиты информации от несанкционированного доступа: идентификация и аутентитфикация, разграничением доступа, контроль целостно-

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			сти, регистрация событий и т.д. Программные средства защиты информации от несанкционированного доступа. Программно-аппаратные средства защиты информации от несанкционированного доступа.
	10.	2	**Методы и средства криптографической защиты информации** Термины и определения в области криптографии. Классификация криптографических средств. Основные методы шифрования.
	11.	2	**Организация защиты информации на объектах информатизации** Организация защиты информации на объектах информатизации. Аттестация объектов информатизации по требованиям безопасности информации.
2	12.	2	**Информационное противоборство (информационная война)** Содержание информационного противоборства на межгосударственном уровне. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.
	13.	2	**Информационная безопасность в системе национальной безопасности Российской Федерации.** Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Информационная безопасность РФ (определение). Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Угрозы информационной безопасности РФ в информационной сфере. Направления обеспечения информационной безопасности государства. Государственная система защиты информации.
	14.	2	**Нормативные правовые акты в области информационной безопасности и защиты информации.** Структура нормативных правовых актов в области информационной безопасности и защиты информации. Федеральные законы и указы Президента РФ. Постановления правительства РФ. Национальные стандарты и ГОСТы. Нормативные и методические документы ФСТЭК России и ФСБ России
	15.	2	**Лицензирование деятельности в области информационной безопасности, сертификация средств защиты информации.** Лицензировании деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну. Лицензирование деятельности по технической защите информации. Лицензирование деятельности по использованию криптографических

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
			средств защиты информации. Лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, Сертификация средств защиты информации.
	16.	2	**Подготовка кадров в области информационной безопасности в Российской Федерации.** Система подготовки кадров в области информационной безопасности в Российской Федерации. Профессиональные стандарты в области информационной безопасности. Федеральные государственные стандарты высшего образования по направлению «Информационная безопасность». Учебный план подготовки бакалавров по направлению 10.03.01 «Информационная безопасность» и профилю «Техническая защита информации»

4.2. Практические занятия (семинары)

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
1	1	4	**Угрозы безопасности информации.** Информация – как объект защиты: Информация - как объект защиты. Виды защищаемой информации. Угрозы безопасности информации: Свойства безопасности информации. Угрозы безопасности информации. Классификация угроз безопасности информации. Разглашение сведений. Перехват информации техническими средствами. Несанкционированный доступ к информации. Угрозы целостности и доступности информации. Уголовная и административная ответственность за реализацию угроз безопасности информации
	2	4	**Основные направления и задачи защиты информации.** Цели и основные направления защиты информации: Защита информации - определение. Основные задачи защиты информации Основные направления защиты информации (определение, способы, средства): организационно-правовая защита информации, техническая защита информации (защита информации от несанкционированного доступа и несанкционированного воздействия, защита информации от утечки по техническим каналам, защита информации от разглашения), криптографическая защита информации, физическая защита объектов информатизации.

2	3	4	**Информационная безопасность в системе национальной безопасности Российской Федерации.** Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Информационная безопасность РФ (определение). Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Угрозы информационной безопасности РФ в информационной сфере. Направления обеспечения информационной безопасности государства. Государственная система защиты информации.
	4	4	**Подготовка кадров в области информационной безопасности в Российской Федерации.** Система подготовки кадров в области информационной безопасности в Российской Федерации. Направления (специальности) подготовки в области информационной безопасности. ФГОС ВО по направлению подготовки «Информационная безопасность». Профессиональные стандарты в области информационной безопасности. Требования профессионального стандарта «Специалист по технической защите информации»: обобщенные трудовые функции, трудовые функции, трудовые действия. Требования федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация «бакалавр»): универсальные, общепрофессиональные, профессиональные компетенции.

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	6	**Подготовка к практическому занятию № 1:** Изучение материалов лекции №№ 1-5 и рекомендованной литературы. Изучение плана проведения семинара № 1. Подготовка доклада и презентации по одному из вопросов семинара

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	6	**Подготовка к практическому занятию № 2:** Изучение материалов лекции №№ 6 - 11 и рекомендованной литературы. Изучение плана проведения семинара № 2. Подготовка доклада и презентации по одному из вопросов семинара
2	6	**Подготовка к практическому занятию № 3:** Изучение материалов лекции №№ 12 - 15 и рекомендованной литературы. Изучение плана проведения семинара № 3. Подготовка доклада и презентации по одному из вопросов семинара
	6	**Подготовка к практическому занятию № 4:** Изучение материалов лекции № 16 и рекомендованной литературы. Изучение плана проведения семинара № 4. Подготовка доклада и презентации по одному из вопросов семинара
1,2	16	**Подготовка реферата**
1,2	8	**Подготовка к сдаче зачета** Изучение материалов лекции №№ 1 - 16 и рекомендованной литературы.

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

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. Угрозы безопасности информации, цели и задачи защиты информации.

Тексты лекций № 1 – 11. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинарских занятий № 1 и 2. ОРИОКС// URL: http://orioks.miet.ru/

Методические указания по подготовке рефератов. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Информационная безопасность Российской Федерации.

Тексты лекций № 12 – 16. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинарских занятий № 3 и 4. ОРИОКС// URL: http://orioks.miet.ru/

Методические указания по подготовке рефератов. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Бутакова Н.Г. Криптографические методы и средства защиты информации : Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ "Интермедия", 2017. - 384 с. - ISBN 978-5-4383-0135-6 .-Текст- непосредственный.
2. Введение в информационную безопасность : Учеб. пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев [и др.]; Под ред. В.С. Горбатова. - М. : Горячая линия-Телеком, 2011. - 288 с. - URL: https://e.lanbook.com/book/5171 (дата обращения: 15.03.2021). - ISBN 978-5-9912-0160-5.
3. Коваленко Ю.И Правовой режим лицензирования и сертификации в сфере информационной безопасности : Учеб. пособие / Ю.И. Коваленко. - М. : Горячая линия-Телеком, 2012. - 140 с. - URL: https://e.lanbook.com/book/5163 (дата обращения: 15.03.2021). - ISBN 978-5-9912-0261-9.
4. 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. - Текст : электронный.
5. 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.
6. 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 издания. - ISBN 978-5-7256-0733-8 .
7. 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. - Имеется электронная версия издания. - ISBN 978-5-7256-0738-3 .
8. Галатенко В.А. Основы информационной безопасности : Учеб. пособие / В.А. Галатенко. - 2-е изд. - М. : ИНТУИТ, 2016. - 266 с. - URL: https://e.lanbook.com/book/100295 (дата обращения: 15.03.2021). - ISBN 978-5-94774-821-5 .
9. Воеводин, В.А. Правовые основы аудитанформационной 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.
10. 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.
11. 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.

12. 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 .

13. 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 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.

2. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации

3. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения.

4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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.

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).

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	1. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	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.	– 28 шт. 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информационно - технологическая платформа ОРИОКС – 28 шт.
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее место преподавателя (АРМ-П) – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С) – 27 шт.	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

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-1. ОИБ «Способен оценивать роль информации и информационной безопасности в современном обществе».

Фонд 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. Информация – как объект защиты.
2. Сведения, составляющие государственную тайну.
3. Персональные данные.
4. Служебная тайна.
5. Коммерческая тайна.
6. Свойства информации.
7. Разглашение сведений ограниченного доступа.
8. Несанкционированный доступ к информации.
9. Перехват информации техническими средствами (утечка информации по техническим каналам).
10. Основные направления и задачи защиты информации.
11. Организационно - правовая защита информации.
12. Защита информации от несанкционированного доступа.
13. Защита информации от утечки по техническим каналам.
14. Криптографическая защита информации.
15. Физическая защита объектов информатизации.
16. Информационная война и информационная безопасность.
17. Информационное оружие.

18. Информационная безопасность в системе национальной безопасности Российской Федерации.
19. Доктрина информационной безопасности Российской Федерации.
20. Основные угрозы информационной безопасности Российской Федерации.
21. Стратегические цели обеспечения информационной безопасности.
22. Состояние информационной безопасности в области обороны страны.
23. Состояние информационной безопасности в области государственной и общественной безопасности.
24. Состояние информационной безопасности в экономической сфере.
25. Состояние информационной безопасности в области науки.
26. Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства.
27. Направления обеспечения информационной безопасности Российской Федерации.
28. Государственная система защиты информации.
29. Государственная система подготовки кадров в области информационной безопасности.
30. Федеральные образовательные стандарты в области информационной безопасности.
31. Профессиональные образовательные стандарты в области информационной безопасности.
32. Федеральные законы в области информационной безопасности и защиты информации.
33. Постановления правительства в области информационной безопасности и защиты информации.
34. Национальные стандарты в области информационной безопасности и защиты информации.
35. Международные стандарты в области информационной безопасности и защиты информации.
36. ГОСТы в области информационной безопасности и защиты информации.
37. Нормативные и методические документы ФСТЭК России в области информационной безопасности и защиты информации.
38. Нормативные и методические документы ФСБ России в области информационной безопасности и защиты информации.
39. Лицензирование деятельности в области технической защиты информации.
40. Лицензировании деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну.
41. Лицензирование деятельности по использованию криптографических средств защиты информации.
42. Лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации.
43. Сертификация средств защиты информации.

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 терми-

ны 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 (выступление на семинарах, сдача реферата), посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача зачета) 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.

Таблице 11.1.

Структура и график контрольных мероприятий

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
4	Семинар № 1	12	6
8	Семинар № 2	12	6
12	Семинар № 3	12	6
16	Семинар № 4	12	6
16	Посещаемость, активность	4	2
16	Реферат	24	12
	Итого за текущий контроль	***76***	***38***
17	***Итоговый контроль***	***24***	***12***
	Накопленный рейтинг	**100**	**50**

Текущая аттестация по дисциплине (итоговый контроль) осуществляется в виде **зачета**.

К зачету допускаются студенты, выполнившие все требования учебной программы и выполнившие все тесты и контрольные мероприятия.

Оценка за дисциплину («зачет» или «незачет») выставляется на основании положения «О накопительной, балльной системе оценки знаний студентов». Для получения зачета студенту необходимо набрать не менее 50 баллов.

Положительная оценка («зачет») заносится в зачетную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» («незачет») проставляется только в зачетную ведомость.

РАЗРАБОТЧИК

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

Рабочая программа дисциплины «Основы информационной безопасности» 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 /