Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Беспалов Владимир Александрович
Должность: Ректор МИЭТ
Дата подписания: 01.09.2023 14:12:11
Уникальный программный ключ:
ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f736d76c8f8bea882b8d602

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
«Проектирование систем защиты объектов информатизации»
(деловая игра)

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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 021B3F91004AAD61874DBC90987DB30618
Владелец: Беспалов Владимир Александрович
Действителен: с 17.06.2021 до 17.06.2022

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.ПСЗОИ. Способен применять нормативные правовые акты, нормативные и методические документы при проектировании систем защиты объектов информатизации	**Знания:** требования нормативных и методических документов ФСТЭК России по защите информации на объектах информатизации (ОИ); порядок организации работ по созданию системы защиты информации (СЗИ) ОИ; порядок разработки и содержание технического задания на создание СЗИ ОИ; структуру и порядок подготовки конкурсной документации на создание системы защиты информации ОИ. этапы проектирования СЗИ ОИ; порядок разработки и содержание технического проекта СЗИ ОИ. **Умения:** проводить анализ угроз безопасности информации, разрабатывать модели угроз безопасности информации; организовать работу коллектива по проектированию системы защиты информации объекта информатизации; **Опыт практической деятельности:** проектирования комплексной системы защиты объекта информатизации; обоснования структуры комплексной системы защиты объекта информатизации; организации выполнения работ, управления коллективом исполнителей и принятия управленческих решений.
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для	ОПК-12.ПСЗОИ Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты	**Знания:** порядок организации работ по созданию системы защиты информации ОИ; методы и этапы проектирования комплексной системы защиты информа-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
технико-экономического обоснования соответствующих проектных решений.	информации	ции ОИ; структуру и порядок подготовки конкурсной документации на создание системы защиты информации ОИ. основные принципы организации технического, программного и информационного обеспечения ОИ; методику обоснования функциональной и организационной структуры системы защиты информации ОИ, а также разработки её архитектуры; методы обеспечения информационной безопасности при создании системы защиты информации ОИ; **Умения:** проводить предпроектное обследование ОИ; проводить анализ требований к СЗИ ОИ в соответствии с уровнем конфиденциальности обрабатываемой информации; разрабатывать проекты технического задания на СЗИ ОИ; разрабатывать конкурсную документации на разработку СЗИ ОИ; разрабатывать технические проекты СЗИ ОИ. **Опыт практической деятельности:** проектирования систем защиты информации объектов информатизации.

В результате изучения дисциплины студент должен:

Знать:

требования нормативных и методических документов ФСТЭК России по защите информации на объектах информатизации (ОИ);

порядок организации работ по созданию системы защиты информации (СЗИ) ОИ;

порядок разработки и содержание технического задания на создание СЗИ ОИ;

структуру и порядок подготовки конкурсной документации на создание системы защиты информации ОИ.

этапы проектирования СЗИ ОИ;

порядок разработки и содержание технического проекта СЗИ ОИ.

Уметь:

проводить предпроектное обследование ОИ;

проводить анализ требований к СЗИ ОИ в соответствии с уровнем конфиденциальности обрабатываемой информации;

разрабатывать проекты технического задания на СЗИ ОИ;

разрабатывать конкурсную документации на разработку СЗИ ОИ;

разрабатывать технические проекты СЗИ ОИ.

Иметь опыт практической деятельности:

проектирования систем защиты информации объектов информатизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Проектирование систем защиты объектов информатизации (деловая игра)» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 4-м курсе в 8-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», «Основы управления информационной безопасностью», «Физическая защита объектов информатизации».

Знания и умения, полученные в результате изучения дисциплины, используются 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	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практическая подготовка при проведении практических занятий	Групповые		
4	8	3	108	60	-	-	48	12	48	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Лабораторные работы	Практическая подготовка при проведении практических занятий	Групповые консультации		
1. Организация и сопровождение закупки услуги по проектированию системы защиты информации объекта информатизации	-	-	24	6	24	Зачет по ПЗ № 1-6 Отчёт по модулю №1
2. Разработка технического проекта системы защиты информации объекта информатизации	-	-	24	6	24	Зачет по ПЗ № 7-12 Отчёт по модулю №2

4.1. Лекционные занятия

Не предусмотрены

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
1	1.	4	Практическое занятие - групповое упражнение. Тема: Инициирование процедуры проектирования системы защиты информации ОИ.
	2.	4	Практическое занятие - групповое упражнение. Тема: Предпроектное обследование объекта информатизации (ОИ).
	3.	4	Практическое занятие - групповое упражнение. Тема: Анализ требований к системе защиты информации ОИ в соответствии с уровнем конфиденциальности обрабатываемой информации.
	4.	4	Практическое занятие - групповое упражнение. Тема: Разработка технического задания на систему защиты информации ОИ
	5.	4	Практическое занятие - групповое упражнение. Тема: Практическое занятие - групповое упражнение. Тема: Разработка конкурсной документации на разработку системы защиты информации ОИ.
	6.	4	Практическое занятие - групповое упражнение. Тема: Организация и сопровождение закупки услуги по проектированию системы защиты информации ОИ.

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
2	7.	4	Практическое занятие - групповое упражнение. Тема: Организация проектирования системы защиты информации ОИ.
	8.	4	Практическое занятие - групповое упражнение. Тема: Разработка эскизного проекта подсистемы защиты информации от несанкционированного доступа ОИ.
	9.	4	Практическое занятие - групповое упражнение. Тема: Разработка эскизного проекта подсистемы защиты информации от утечки по техническим каналам ОИ.
	10.	4	Практическое занятие - групповое упражнение. Тема: Разработка эскизного проекта подсистемы физической защиты ОИ
	11.	4	Практическое занятие - групповое упражнение. Тема: Разработка технического проекта системы защиты информации ОИ.
	12.	4	Практическое занятие - групповое упражнение. Тема: Защита технического проекта на создание системы защиты информации ОИ.

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 практическому занятию № 1:** Изучение методических рекомендаций по проведению ПЗ № 1 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 2:** Изучение методических рекомендаций по проведению ПЗ № 2 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 3:** Изучение методических рекомендаций по проведению ПЗ № 3 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 4:** Изучение методических рекомендаций по проведению ПЗ № 4 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 5:** Изучение методических рекомендаций по проведению ПЗ № 5 и рекомендованной литературы

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	4	**Подготовка к практическому занятию № 6:** Изучение методических рекомендаций по проведению ПЗ **№** 6 и рекомендованной литературы
2	4	**Подготовка к практическому занятию № 7:** Изучение методических рекомендаций по проведению ПЗ № 7 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 8:** Изучение методических рекомендаций по проведению ПЗ **№** 8 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 9:** Изучение методических рекомендаций по проведению ПЗ **№** 9 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 10:** Изучение методических рекомендаций по проведению ПЗ № 10 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 11:** Изучение методических рекомендаций по проведению ПЗ № 11 и рекомендованной литературы
	4	**Подготовка к практическому занятию № 12:** Изучение методических рекомендаций по проведению ПЗ № 12 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. Организация и сопровождение закупки услуги по проектированию системы защиты информации объекта информатизации.

Информационно-справочный материал к практическим занятиям № 1 – 6. ОРИОКС// URL: http://orioks.miet.ru/

Методические рекомендации студентам по подготовке и проведению практических занятий № 1 – 6. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Разработка технического проекта системы защиты информации объекта информатизации.

Информационно-справочный материал к практическим занятиям № 7 – 12. ОРИОКС// URL: http://orioks.miet.ru/

Методические рекомендации студентам по подготовке и проведению практических занятий № 7 – 12. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

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. 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. - 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 - Текст : непосредственный.
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: 16.03.2021). - 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 безопасности 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 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.

5. 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.

6. 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.-URL: https://docs.cntd.ru/document/1200084141 (дата обращения 15.03.2021).- Текст: электронный.

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 технических 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. -URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 16.03.2021) -Текст: электронный.

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.

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.

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).-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 - . - 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.

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 под-	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	ключения к сети Интернет и обеспечением доступа в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	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 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):	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
	ПЭВМ Flagman-G в составе: 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.ПСЗОИ. Способен применять нормативные правовые акты, нормативные и методические документы при проектировании систем защиты объектов информатизации.

ФОС по подкомпетенции ОПК-12.ПСЗОИ 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

11.1. Особенности организации процесса обучения

В целях практической подготовки в дисциплине предусмотрены практические занятия-групповые упражнения.

Каждое практическое занятие-групповое упражнение направлены на формирование отдельных умений, необходимых для формирования общепрофессиональных компетенции.

Основные дидактические цели деловой игры и мотивация студентов достигаются антагонистической атмосферой («Заказчики» критически оппонируют «Исполнителям», а также соревновательностью между подгруппами «Исполнителей».

Для достижения дидактических целей и решения частных задач формирования компетенций у студентов в рамках деловой игры учебная группа делится на подгруппы «Заказчиков» и подгруппы «Исполнителей», что позволяет осуществить максимальный охват студентов заданиями различных направлений деятельности и по всем темам занятий.

На каждое занятие руководитель занятия, выполняющий роль в том числе и посредника в деловой игре, доводит целевую установку и ставит задание в рамках структурно-логической схемы прохождения игры каждой подгруппе.

Руководители подгрупп, назначаемые из числа студентов, распределяют задание между студентами подгруппы таким образом, чтобы в процессе подготовки к практическому за-

нятию каждый студент подгруппы смог бы подготовить свое задание по каждой теме и доложить полученные результаты в ходе выступления на деловой игре.

На практическом занятии под руководством преподавателя студенты каждой из подгрупп «Исполнителей» по очереди докладывают свои принятые решения и защищают их. Студенты подгруппы «Заказчиков» в соответствии с распределенными ролями и направлениями принимают работу «Исполнителей», уточняют непонятные вопросы, делают замечания. В случае недостаточной проработки вопроса студентами преподаватель вмешивается в процесс совещания, уточняет и корректирует работу «Заказчиков».

11.2. Методические указания студентам по подготовке к практическим занятиям

Перед каждым практическим занятием студенты на сайте МИЭТ в ОРИОКС должны ознакомиться с информационно-справочными материалами к занятию.

В соответствие с полученным от руководителя группы заданием студент должен разработать соответствующие документы, подготовить презентацию для доклада и обсудить данные материалы с коллегами по группе.

По итогам отработки всех практических занятий каждый студент формирует сводный отчет о проделанной работе в рамках деловой игры который должен включать:

- тему каждого занятия,
- роль студента на занятии,
- соответствующим образом оформленные документы, разработанные лично студентом к занятию с учетом сделанных при докладе (защите) замечаний на каждом занятии,
- описание личного вклада студента и собственной оценки достижения целей студентом на занятии,
- общий вывод по результатам деловой игры и рекомендации по совершенствованию формы и содержания отрабатываемых на деловой игре вопросов.

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 (защита отчетов по практическим занятиям),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 – $R_{нор}$).

Примерные структура и графики контрольных мероприятий приведены в таблице ниже.

Структура и график контрольных мероприятий

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
1	Практическое занятие № 1	4	2
2	Практическое занятие № 2	4	2
3	Практическое занятие № 3	4	2
4	Практическое занятие № 4	8	4
5	Практическое занятие № 5	4	2

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
6	Практическое занятие № 6	4	2
7	Практическое занятие № 7	4	2
8	Практическое занятие № 8	4	2
9	Практическое занятие № 9	4	2
10	Практическое занятие № 10	4	2
11	Практическое занятие № 11	4	2
12	Практическое занятие № 12	8	4
13	Посещаемость, активность	14	7
	Итого за текущий контроль	***70***	***35***
	Итоговый контроль	***30***	***15***
	Накопленный рейтинг	**100**	**50**

В зачетную ведомость и зачетную книжку вносится не зачетная 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

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 «Проектирование систем защиты объектов информатизации (деловая игра)» 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 /