Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гаврилов Сергей Александрович
Должность: Ректор
Дата подписания: 14.10.2026 15:37:40
Уникальный программный ключ:
488ddcd30399efca200d034e027f45455f6eb1b9

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.Г. Балашов
«16» мая 2025 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Для всех направлений и направленностей (профилей) бакалавриата

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 009BD2B5B7DC0794F9C207D6C8F586BD59
Владелец ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ "МОСКОВСКИЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ"
Действителен с 16.06.2026 по 09.09.2027

Москва 2025

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

Компетенции ОП	**Подкомпетенции, формируемые в дисциплине**	**Индикаторы достижения компетенций**
Направление 12.03.04 Биотехнические системы и технологии Направленность (профиль) «Биомедицинские электронные и компьютерные системы»		
ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	**ОПК-4.ОИБ** Способен соблюдать основные требования информационной безопасности при решении задач профессиональной деятельности.	**Знания**: - теоретических основ информационной безопасности. **Умения**: - применять методы и средства защиты информации. **Опыт:** - организации защиты информации с соблюдением основных требований к информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программ.

Входные требования к дисциплине - знает современные программные средства для создания и редактирования текстов, изображений;

знает современные принципы поиска, хранения, обработки, анализа и представления в требуемом формате информации;

умеет решать задачи обработки данных с помощью современных средств информатизации;

использует информационно-коммуникационные технологии при поиске необходимой информации;

использует информационно-коммуникационные технологии для подготовки документации.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа			Самостоятельная работа (часы)	Промежуточная аттестация
				Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
Направление 12.03.04 Биотехнические системы и технологии Направленность (профиль) «Биомедицинские электронные и компьютерные системы»								
4	7	3	108	32	0	16	60	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1. Угрозы безопасности информации	14	-	4	10	Контроль результатов СРС к практическому занятию 1 в форме докладов.
					Тестирование 1.
2. Способы и средства защиты информации. Организация защиты информации	18	-	12	50	Контроль результатов СРС к практическому занятию 2-4 в форме докладов.
					Защита домашних заданий 1-4.
					Тестирование 2.

4.1. Лекционные занятия

№ модуля дисциплины	№ 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.	4	**Классификация угроз безопасности информации.** Объекты защиты (объект информатизации, выделенное помещение, автоматизированная система, информационная система, 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 нарушение безопасности информации.
	3.	2	**Технические каналы утечки информации. 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 информации. Технические каналы утечки акустической речевой информации.** 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.	4	**Способы и средства несанкционированного доступа к информации и несанкционированного воздействия на информацию**. Классификации способов несанкционированного доступа к информации (НСД). Программные способы с средства НСД. Программно-технические способы и средства НСД. Способы удаленного доступа к компьютеру по сети. Типовые программы для контроля действий пользователей в локальной компьютерной сети и программ – шпионов. Классификация и основные возможности нарушителей НСД.

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
			Классификация способов несанкционированного воздействия на информацию (НСВ). Вредоносные программы (программные закладки, классические программные (компьютерные) вирусы, вредоносные программы, распространяющиеся по сети (сетевые черви), недекларированные возможности программного обеспечения). Основные виды вредоносных программ. Основные деструктивные действия, выполняемыми вирусами. Типовые вредоносные программы. Разновидности угроз НСВ на сетевом уровне. Причины непреднамеренного несанкционированного воздействия на информацию.
2	6.	2	**Основные направления защиты информации.** Защита информации - определение. Виды (направления) защиты информации (организационно-правовая защита информации, техническая защита информации, криптографическая защита информации, физическая защита объектов информатизации, защита информации от разглашения). Задачи защиты информации. Лицензирование деятельности в области защиты информации. Ответственность за незаконную деятельность по защите 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.	4	**Способы и средства защиты информации от**

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
			несанкционированного доступа. Классификация способов защиты информации от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации. Классификация средств вычислительной техники и требования по защите информации Классификация средств межсетевого экранирования для автоматизированных систем и требования по защите информации. Классификация систем и средств защиты информации от НСД. Технологии защиты информации от НСД. Типовые системы и средства защиты АС от несанкционированного доступа. Межсетевые экраны.
	10.	2	**Методы и средства антивирусной защиты.** Методы обнаружения вирусов. Антивирусные программы. Средства обнаружения атак на сетевом уровне.
	11.	2	**Методы и средства криптографической защиты информации.** Термины и определения в области криптографической защиты информации. Криптографические методы преобразования информации. Классификация методов шифрования информации. Симметричные криптосистемы. Криптосистемы с открытым ключом. Классификация и характеристика криптографических средств.
	12.	4	**Организация защиты информации на предприятии** Порядок организации защиты информации на предприятии. Определение перечня сведений конфиденциального характера. Разработка модели угроз безопасности информации. Обоснование требований к системе защиты информации. Разработка технического задания на создание системы защиты информации. Проектирование системы защиты информации. Внедрение системы защиты информации. Организационно-распорядительные документы по защите информации, разрабатываемые на предприятии. Аттестация объектов информатизации по требованиям безопасности информации.

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование занятия
1	1-2	4	**Практическое занятие (семинар) № 1**. Угрозы безопасности информации.
2	3-4	4	**Практическое занятие (семинар) № 2**. Способы и средства защиты информации от утечки по техническим каналам.
2	5-6	4	**Практическое занятие (семинар) № 3**. Способы и средства защиты информации от несанкционированного доступа.
2	7-8	4	**Практическое занятие (семинар) № 4**. Организация защиты информации на предприятии.

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	4	Подготовка к практическому занятию №1. Изучение материалов лекций №№1-5 и рекомендованной литературы. Изучение плана проведения практического занятия №1. Подготовка доклада по одному из вопросов.
1	5	Подготовка к Тестированию 1. Изучение материалов лекций №№1-5, изучение материалов по практическому занятию 1 и рекомендованной литературы.
1	1	Тестирование 1. Прохождение электронного тестирования по модулю 1.
2	4	Подготовка к практическому занятию № 2. Изучение материалов лекций №№ 6-8 и рекомендованной литературы. Изучение плана проведения практического занятия №2. Подготовка доклада по одному из вопросов.
2	4	Подготовка к практическому занятию № 3. Изучение материалов лекций №№ 9-11 и рекомендованной литературы.

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
		Изучение плана проведения практического занятия №3. Подготовка доклада по одному из вопросов.
2	8	Выполнение домашнего задания №1. Настройка штатных средств защиты информации в ОС. Подготовка отчета.
2	8	Выполнение домашнего задания №2. Установка и настройка средств антивирусной защиты и средства сетевой безопасности компьютера
2	8	Выполнение домашнего задания №3. Установка и настройка средств криптографической защиты информации. Подготовка отчета.
2	8	Выполнение домашнего задания №4. Установка и настройка средств резервного копирования, восстановления данных и гарантийного уничтожения информации. Подготовка отчета.
2	4	Подготовка к практическому занятию №4. Изучение материалов лекции №№12 и рекомендованной литературы. Изучение плана проведения практического занятия №4. Подготовка доклада по одному из вопросов.
2	5	Подготовка к Тестированию 2. Изучение материалов лекций №№ 6-12 и рекомендованной литературы.
2	1	Тестирование 2. Прохождение электронного тестирования по модулю 2.

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// URL: http://orioks.miet.ru/).

Материалы для изучения теории в рамках подготовки к практическим занятиям размещены в ОРИОКС: текст основных теоретических сведений, задания для СРС и критерии их оценивания, рекомендуемая литература в файле: «Методические указания для студентов по изучению дисциплины «Основы информационной безопасности».

Модуль 1 «Угрозы безопасности информации»:

–материалы для подготовки к тестированию: тексты лекций, презентация к лекциям, учебная литература по дисциплине;

–материалы для подготовки к практическому занятию №1: план проведения практического занятия, методические рекомендации по подготовке доклада, учебная литература к практическому занятию;

–онлайн тестирование 1.

Модуль 2 «Способы и средства защиты информации. Организация защиты информации»:

–материалы для подготовки к тестированию: тексты лекций, презентация к лекциям, учебная литература по дисциплине;

–материалы для подготовки к практическому занятию №2: план проведения практического занятия, методические рекомендации по подготовке доклада, учебная литература к практическому занятию;

–материалы для подготовки к практическому занятию №3: план проведения практического занятия, методические рекомендации по подготовке доклада, учебная литература к практическому занятию;

–материалы для подготовки к практическому занятию №4: план проведения практического занятия, методические рекомендации по подготовке доклада, учебная литература к практическому занятию;

–материалы для выполнения домашнего задания: методические рекомендации по проведению домашних заданий №1-4 (перечень используемого программного обеспечения, учебная литература, краткие теоретические сведения, порядок выполнения практической части, контрольные вопросы), форма отчета по результатам проведения домашнего задания №1-4;

–онлайн тестирование 2;

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Петренко, В. И. Защита персональных данных в информационных системах. Практикум / В. И. Петренко, И. В. Мандрица. – 4-е изд., стер. – Санкт-Петербург : Лань, 2022. – 108 с. – URL: https://e.lanbook.com/book/264242 (дата обращения: 15.06.2025).
2. 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. – Имеется электронная версия издания. – ISBN 978-5-7256-0972-1
3. 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. – Имеется электронная версия издания. – ISBN 978-5-7256-0961-5
4. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: https://doi.org/10.29039/02005-0. - ISBN 978-5-369-02005-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233509 (дата обращения: 15.06.2025). – Режим доступа: по подписке.
5. Бирюков, А. А. Информационная безопасность. Защита и нападение : практическое руководство / А. А. Бирюков. – 3-е изд., перераб. и доп. - Москва : ДМК Пресс, 2023. - 442 с. – ISBN 978-5-93700-219-8. - Текст : электронный. - URL: https://e.lanbook.com/book/455351 (дата обращения: 15.06.2025). – Режим доступа: по подписке.
6. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. - Москва : Форум, 2022. - 592 с. - (Высшее образование:

Бакалавриат). - URL: https://znanium.com/catalog/product/1843022 (дата обращения: 15.06.2025). - ISBN 978-5-8199-0730-6

7. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 (дата обращения: 15.06.2025). — Режим доступа: для авториз. пользователей.

8. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. – 3-е изд., перераб. и доп. – М.: Юрайт, 2026. – 161 с. – (Высшее образование). – URL: https://urait.ru/bcode/584050 (дата обращения: 15.06.2025). – ISBN 978-5-534-07248-8.

9. Организационное и правовое обеспечение информационной безопасности : Учебник для вузов / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов ; Под ред. Т. А. Поляковой, А. А. Стрельцова. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2026. – 357 с. – (Высшее образование). – URL: https://urait.ru/bcode/583236 (дата обращения: 15.06.2025). - ISBN 978-5-534-19108-0

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.

Периодические издания

1. ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ : научный журнал / Научно-производственное объединение Эшелон. - Москва : НПО Эшелон, 2013. - URL: https://elibrary.ru/title_about_new.asp?id=50036 (дата обращения: 15.06.2025). - Режим доступа: для зарегистрированных пользователей. - URL: https://cyberrus.info/ (дата обращения: 12.05.2025). - Режим доступа: свободный. - ISSN 2311-3456. - Текст : электронный.

2. ВЕСТНИК УРФО. БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СФЕРЕ : научный журнал / ФГАОУ ВО Южно-Уральский государственный университет (национальный исследовательский университет). - Челябинск : ЮУрГУ, 2011. - URL: http://www.info-secur.ru/index.php/ojs (дата обращения: 15.06.2025). - Режим доступа: свободный. - URL: https://www.susu.ru/ru/science/journals (дата обращения: 15.06.2025). - URL: https://www.elibrary.ru/title_about_new.asp?id=32751 (дата обращения: 15.06.2025). - Режим доступа: для зарегистрированных пользователей. - ISSN 2225-5435 (Print); 2225-5443 (Online). - Текст : электронный.

3. INFORMATION SECURITY/ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ : профессиональное издание / Компания ГРОТЕК. - Москва : ГРОТЕК, [2005]. - URL: https://lib.itsec.ru/imag/ (дата обращения: 15.06.2025). - Режим доступа: свободный. - Текст : электронный.

4. ЗАЩИТА ИНФОРМАЦИИ. ИНСАЙД : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004. - URL: https://lib.rucont.ru/efd/909910/info (дата обращения: 15.06.2025). - Режим доступа: по подписке (2026-). - URL: https://eivis.ru/browse/publication/122426 (дата обращения: 15.06.2025). - Режим доступа: по подписке (2020-2025). - URL: https://www.elibrary.ru/title_about_new.asp?id=25917 (дата обращения: 15.06.2025). - Режим доступа: по подписке (2017-2023). - ISSN 2413-3582. - Текст : электронный.

5. 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: 15.06.2025). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

6. JET INFO : деловое издание. - Москва : Компания "Инфосистемы Джет", 1995. - URL: http://www.jetinfo.ru/ (дата обращения: 15.06.2025). - Режим доступа: свободный. - Текст : электронный.

7. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994. - URL: https://bit.spels.ru/index.php/bit (дата обращения: 15.06.2025). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. – URL: https://www.elibrary.ru (дата обращения: 15.06.2025). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – URL: https://e.lanbook.com (дата обращения: 15.06.2025). – Текст: электронный.

3. Znanium: электронно-библиотечная система: сайт. – URL: https://znanium.ru/ (дата обращения: 15.06.2025). – Текст: электронный.

4. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 15.06.2025). – Текст: электронный.

5. ФСТЭК России: Банк данных угроз безопасности информации. – URL: https://bdu.fstec.ru/ (дата обращения: 15.06.2025). – Текст: электронный.

6. Бюро научно-технической информации «Техника для спецслужб». – URL: http://www.bnti.ru/about.asp (дата обращения: 15.06.2025). – Режим доступа: свободный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используются смешанное обучение, основанное на интеграции технологий традиционного и электронного обучения. Часть учебных занятий проходит с использованием взаимодействия студентов и преподавателя в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы, размещенные в электронной информационно-образовательной среде ОРИОКС (http://orioks.miet.ru): электронные версии лекций, практических занятий, домашних заданий, методических разработок по тематике курса, тестирования и др.

Тестирования проводятся в ОРИОКС.

В сервисе обратной связи ОРИОКС «Домашние задания» обучающиеся выкладывают на проверку выполненные практические задания и домашние задания, а также могут задавать уточняющие вопросы преподавателю.

Для взаимодействия студентов с преподавателем используются дополнительные сервисы обратной связи: электронная почта кафедры ib.labs@yandex.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	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).
Компьютерный класс	Компьютеры, мультимедийное оборудование	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).
Лаборатория технологий и управления информационной безопасности	1. Автоматизированное рабочее место преподавателя (АРМ-П) в составе ПЭВМ, мультимедийного проектора, экрана – 1 комплект. 2. АРМ слушателей (АРМ-С) с программным обеспечением для обработки и защиты данных, возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду МИЭТ – 27 комплектов. 3. Серверное и сетевое оборудование – 1 комплект.	Microsoft Windows, Microsoft Office, браузер Антивирус (Касперского/DrWeb/EsetNod32 /Microsoft Security Essentials/ Avast) Oracle VM VirtualBox, Cisco_Packet_Tracer (доступ с удаленного рабочего стола).
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ ОРИОКС	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции **ОПК-4.ОИБ** «Способен соблюдать основные требования информационной безопасности при решении задач профессиональной деятельности».

Фонд оценочных средств представлен 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

Для формирования подкомпетенции и приобретения необходимых знаний, умений и опыта в рамках данного курса читаются лекции, проводятся практические занятия.

В процессе изучения курса предполагается самостоятельная работа студента при подготовке к лекционным, практическим занятиям, выполнению домашних и практических заданий, тестов, подготовке докладов. При этом студент использует методические разработки, рекомендуемую литературу, библиотеку электронных модулей в электронной информационной образовательной среде ОРИОКС, информационно-справочные системы.

Максимальная эффективность освоения материалов ***лекций*** достигается при предварительной подготовке к ней. Студенту рекомендуется заранее ознакомиться с предстоящей темой лекции и основными ее тезисами, подготовить вопросы к лектору по заинтересовавшим разделам.

Для закрепления лекционного материала проводятся ***практические занятия***. Для повышения эффективности практических занятий (семинаров) студенту также необходимо предварительно ознакомиться с методическими указаниями, прочитать конспект лекций по данной тематике и соответствующие главы учебника (учебного пособия).

После теоретического рассмотрения материала практического занятия преподаватель выдает каждому студенту практико-ориентированное домашнее задание на применение рассмотренных материалов, которое студенты выполняют в рамках СРС в течение заданного времени. Выполненные задания в виде отчета с выводами по полученным результатам присылаются студентами преподавателю и оцениваются баллами. Оценки доводятся до студентов, при этом может быть организована беседа-дискуссия по разбору итогов выполненной работы и анализу ошибок.

Одной из форм обучения является ***консультация*** у преподавателя. Обращаться к помощи преподавателя следует в любом случае, когда студенту не ясно изложение какого-либо вопроса в учебной литературе или требуется помощь в подборе необходимой дополнительной литературы.

По завершению изучения дисциплины предусмотрен ***экзамен***, при этом оценка итогов учебной деятельности студента основана на балльной накопительной системе. Для итогового контроля по дисциплине разработан ФОС, включающий комплексное профессиональное задание по проверке сформированности необходимой компетенции с методическими указаниями его выполнения и критериями оценки достижения формируемой в дисциплине компетенций/подкомпетенций.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система.

По сумме баллов выставляется итоговая оценка по предмету. Структура и график контрольных мероприятий доступен в ОРИОКС// URL: http://orioks.miet.ru/ .

РАЗРАБОТЧИК:

Профессор кафедры «Информационная безопасность»
доктор технических наук, доцент _____ / А.В. Душкин /

Рабочая программа дисциплины «Основы информационной безопасности» по всем направлениям и направленностям (профилям) бакалавриата разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры «30» июня 2025 года, протокол №6.

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 /