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
«10» января 2024 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Специальность – 38.05.01 «Экономическая безопасность»
Специализация – «Управление экономической безопасностью»

Москва 2024

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.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 деятельности:** - 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 программы.

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)		
4	7	4	144	32	16	16	80	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 и основные направления защиты информации	6	-	4	12	Контроль результатов СРС к практическому занятию 1 в форме докладов. Тестирование 1.
2. Защита информации от несанкционированного доступа	8	16	4	44	Контроль результатов СРС к практическому занятию 2 в форме докладов. Сдача лабораторных работ 1-4. Тестирование 2.
3. Защита информации от утечки по техническим каналам	8	-	4	12	Контроль результатов СРС к практическому занятию 3 в форме докладов. Тестирование 3.
4. Организация и управление информационной безопасностью	10	-	4	12	Контроль результатов СРС к практическому занятию 4 в форме докладов. Тестирование 4.

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	**Угрозы безопасности информации и основные направления защиты информации**		
	1-2	4	**Классификация угроз безопасности информации** Понятие «информация» в области информационной безопасности. Виды информации. Сведения, составляющие государственную тайну. Конфиденциальная информация. Безопасность информации. Свойства безопасности информации. Угроза безопасности информации (определение). Угрозы безопасности информации: утечка информации, неправомерное модификация (искажение, подмена), уничтожение информации, неправомерное блокирование доступа к ней. Виды утечки информации: разглашение сведений, хищение носителя информации, несанкционированный доступ к информации, перехват информации техническими средствами (утечка информации по техническим каналам). Источники угроз безопасности информации.
	3	2	**Основные направления и задачи защиты информации** Защита информации (определение). Основные направление защиты информации. Правовая защита информации. Техническая защита информации. Криптографическая защита информации. Физическая защита объектов информатизации. Основные задачи защиты информации. Уголовная и административная ответственность за разглашение сведений ограниченного доступа и неправомерный доступ к информации. Уголовная и административная ответственность за разглашение сведений ограниченного доступа и неправомерный доступ к информации. Ответственность за незаконную деятельность по защите информации и нарушение правил защиты информации.
2	**Защита информации от несанкционированного доступа**		
	4	2	**Несанкционированный доступ к информации, обрабатываемой АС и СВТ** Несанкционированный доступ к информации (НСД), обрабатываемой автоматизированными системами (АС) и средствами вычислительной техники (СВТ). Классификация способов несанкционированного доступа к информации. Классификация способов несанкционированного воздействия на информацию. Модель нарушителя.
	5	2	**Способы защиты информации от НСД** Классификация способов защиты информации от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации. Межсетевые экраны. Требования по защите информации.

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
	6	2	**Методы и средства криптографической защиты информации** Термины и определения в области криптографии. Классификация криптографических средств. Основные методы шифрования.
	7	2	**Методы и средства антивирусной защиты.** Методы антивирусной защиты. Средства антивирусной защиты.
3	**Защита информации от утечки по техническим каналам**		
	8-9	4	**Классификация и характеристика технических каналов утечки информации.** Классификация и характеристика технических каналов утечки информации, обрабатываемой СВТ. Классификация и характеристика технических каналов утечки акустической речевой информации.
	10	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. Средства защиты объектов информатизации от утечки информации по техническим каналам.
	11	2	**Способы и средства защиты акустической речевой информации от утечки по техническим каналам.** Классификация способов и средств защиты акустической речевой информации от утечки по техническим каналам. Средства защиты акустической речевой информации от утечки по техническим каналам.
4	**Организация и управление информационной безопасностью**		
	12	2	**Организация защиты информации** Общий порядок организации защиты информации. Аналитическое обоснование необходимости создания системы защиты информации (СЗИ). Техническое задание на создание СЗИ
	13-14	4	**Основы проектирования автоматизированных систем в защищенном исполнении** Общие положения о порядке создания автоматизированных систем в защищенном исполнении. Общие и функциональные требования к автоматизированным системам в защищенном исполнении. Типовое содержание работ по защите информации на стадиях создания автоматизированных систем в защищенном исполнении. Особенности испытаний и применения автоматизированной системы в защищенном исполнении.

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
	15-16	4	**Управление информационной безопасностью** Организация управления информационной безопасностью. Политика информационной безопасности. Общие мероприятия по управлению информационной безопасностью. Документы политики информационной безопасности (модель угроз безопасности информации, концепция обеспечения безопасности информации, регламенты обеспечения безопасности информации, инструкции и другие организационно-распорядительные документы по вопросам обеспечения безопасности информации).

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование занятия
1	1	4	**Практическое занятие №1**. Средства и системы обработки данных.
2	2	4	**Практическое занятие №2**. Методы и средства защиты информации от несанкционированного доступа.
3	3	4	**Практическое занятие №3**. Методы и средства защиты информации от утечки по техническим каналам.
4	4	4	**Практическое занятие №4**. Организация и управление информационной безопасностью.

4.3. Лабораторные занятия

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Наименование занятия
2	1	4	**Лабораторная работа 1.** Настройка штатных средств защиты информации в ОС
2	2	4	**Лабораторная работа 2.** Установка и настройка средств антивирусной защиты и средства сетевой безопасности компьютера
2	3	4	**Лабораторная работа 3.** Установка и настройка средств криптографической защиты информации

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Наименование занятия
2	4	4	**Лабораторная работа 4.** Установка и настройка средств резервного копирования, восстановления данных и гарантийного уничтожения информации

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	6	**Подготовка к практическому занятию №1**. Изучение материалов лекции №№1-3 и рекомендованной литературы. Изучение плана проведения семинара №1. Подготовка сообщения по одному из вопросов семинара
1	4	**Подготовка к Тестированию 1.** Изучение материалов лекции №№1-3, изучение материалов по семинару 1 и рекомендованной литературы.
1	2	**Тестирование 1.** Прохождение электронного тестирования по модулю 1.
2	7	**Подготовка к практическому занятию №2**. Изучение материалов лекции №№4-7 и рекомендованной литературы. Изучение плана проведения семинара №2. Подготовка сообщения по одному из вопросов семинара
2	8	**Подготовка к лабораторной работе 1.** Настройка штатных средств защиты информации в ОС Изучение теоретической части лабораторной работы, подготовка отчета по результатам выполнения лабораторной работы.
2	8	**Подготовка к лабораторной работе 2.** Установка и настройка средств антивирусной защиты и средства сетевой безопасности компьютера Изучение теоретической части лабораторной работы, подготовка отчета по результатам выполнения лабораторной работы.
2	8	**Подготовка к лабораторной работе 3.** Установка и настройка средств криптографической защиты информации Изучение теоретической части лабораторной работы, подготовка отчета по результатам выполнения лабораторной работы.
2	8	**Подготовка к лабораторной работе 4.** Установка и настройка средств резервного копирования, восстановления данных и гарантийного уничтожения информации Изучение теоретической части лабораторной работы, подготовка отчета по результатам выполнения лабораторной работы.
2	5	**Подготовка к Тестированию 2.** Изучение материалов лекции №№ 4-7, изучение материалов по семинару 2 и рекомендованной литературы.
2	2	**Тестирование 2.** Прохождение электронного тестирования по модулю 2.

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
3	6	**Подготовка к практическому занятию №3**. Изучение материалов лекции №№8-11 и рекомендованной литературы. Изучение плана проведения семинара №3. Подготовка сообщения по одному из вопросов семинара
3	4	**Подготовка к Тестированию 3.** Изучение материалов лекции №№8-11, изучение материалов по семинару 3 и рекомендованной литературы.
3	2	**Тестирование 3.** Прохождение электронного тестирования по модулю 3.
4	6	**Подготовка к практическому занятию №4**. Изучение материалов лекции №№12-16 и рекомендованной литературы. Изучение плана проведения семинара №4. Подготовка сообщения по одному из вопросов семинара
4	4	**Подготовка к Тестированию 4.** Изучение материалов лекции №№12-16, изучение материалов по семинару 4 и рекомендованной литературы.
4	2	**Тестирование 4.** Прохождение электронного тестирования по модулю 4.

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/).

Методические указания студентам по изучению дисциплины

Модуль 1 «Угрозы безопасности информации и основные направления защиты 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, учебная литература к практическому занятию;

– онлайн тестирование 1.

Модуль 2 «Защита информации от несанкционированного доступа»:

– 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, учебная литература к практическому занятию;

– материалы для подготовки к лабораторным работам: методические рекомендации по проведению лабораторных работ №1-4 (перечень используемого программного обеспечения, учебная литература, краткие теоретические сведения, порядок

выполнения практической части, контрольные вопросы), форма отчета по результатам проведения лабораторных работ №1-4;

– онлайн тестирование 2.

Модуль 3 «Защита информации от утечки по техническим каналам»:

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

– материалы для подготовки к практическому занятию №3: план проведения практического занятия, учебная литература к практическому занятию;

– онлайн тестирование 3.

Модуль 4 «Организация и управление информационной безопасностью»:

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

– материалы для подготовки к практическому занятию №4: план проведения практического занятия, учебная литература к практическому занятию;

– онлайн тестирование 4.

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Программно-аппаратные средства обеспечения информационной безопасности: Учеб. пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. - М. : Горячая линия-Телеком, 2018. - 248 с. - URL: https://e.lanbook.com/book/111053 (дата обращения: 20.06.2023). - ISBN 978-5-9912-0470-5.

2. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. - Москва : Горячая линия-Телеком, 2018. - 586 с. - URL: https://e.lanbook.com/book/111027 (дата обращения: 20.06.2023). - ISBN 978-5-9912-0424-8. - Текст : электронный.

3. 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: 20.06.2023). - ISBN 978-5-507-45301-6. - Текст : электронный.

4. Информационная безопасность: защита и нападение / А. А. Бирюков. - 2-е изд. - Москва : ДМК Пресс, 2017. - 434 с. - URL: https://e.lanbook.com/book/93278 (дата обращения: 20.06.2023). - ISBN 978-5-97060-435-9. - Текст : электронный.

5. Защита информации в информационном обществе / А. А. Малюк. - Москва : Горячая линия-Телеком, 2017. - 230 с. - URL: https://e.lanbook.com/book/111078 (дата обращения: 20.06.2023). - ISBN 978-5-9912-0481-1. - Текст : электронный.

6. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) / В. К. Новиков. - Москва : Горячая линия-Телеком, 2017. - 176 с. - URL: https://e.lanbook.com/book/111084 (дата обращения: 20.06.2023). - ISBN 978-5-9912-0525-2. - Текст : электронный.

Периодические издания

1. Специальная техника / ОАО «Электрозавод». - Москва: Электрозавод, 1998-2017. - В настоящее время не выходит. - URL: https://elibrary.ru/title_about.asp?id=9851 (дата обращения: 20.06.2023). - Режим доступа: по подписке (2014-2017). - ISSN 1996-0506. - Текст : электронный : непосредственный.

2. Защита информации. Inside : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург: ИД Афина, 2004 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=25917 (дата обращения: 20.06.2023). - Режим доступа: по подписке (2017-). - ISSN 2413-3582. - Текст: электронный: непосредственный.

3. 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: 20.06.2023). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст: электронный.

4. Вопросы кибербезопасности: научный журнал / Научно-производственное объединение Эшелон. - Москва: НПО Эшелон, 2013 -. - URL: https://cyberrus.com (дата обращения: 20.06.2023). - Режим доступа: свободный. - ISSN 2311-3456. - Текст: электронный.

5. JET INFO: деловое издание. - Москва: Компания «Инфосистемы Джет», 1995 -. - URL: http://www.jetinfo.ru/ (дата обращения: 20.06.2023). - Режим доступа: свободный. - 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: .03.2021). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.

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

5. Бюро научно-технической информации «Техника для спецслужб». – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – 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.

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, лабораторных работ, 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 лабораторные работы, а также могут задавать уточняющие вопросы преподавателю.

Для взаимодействия студентов с преподавателем используются дополнительные сервисы обратной связи: электронная почта кафедры ib.labs@yandex.ru.

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

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	Специализированная мебель (место преподавателя, посадочные места для студентов) Материально-техническое оснащение: Компьютер, моноблок Lenovo F0AM0092RK, проектор Panasonic PT-VW535N, экран Mediavisor, экран рулонный настенный, телевизор Panasonic TX-85XR940, телевизор LG 55UF771V, клавиатура Lenovo SK-8861, мышь Lenovo ZTM600, радиосистема Shure BLX88E K3E, микрофон GAL VM-175, акустика JBL PRX700, акустика EON15 G , микшер Phonic AM120, HDMI-адаптер Trendnet TU3-HDMI, HDMI-DVB-T Modulator Dr.HD MR 125 HD, коммутатор Eltex MES2208P, учебная доска ,кафедра	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).
Компьютерный класс	Специализированная мебель (место преподавателя, посадочные места для студентов) Материально-техническое оснащение: Моноблок PowerCool AIO V-510, системные блоки A-PC SB-200, мониторы DELL SE2419HR,	Операционная система Microsoft Windows от 7 версии и выше, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Crome); Acrobat reader DC

	комплекты клавиатуры Logitech K120/ мышь Logitech M100, LED телевизор, 65 дюймов, фиксированное настенное крепление с возможностью постинсталляционной регулировки для LCD-телевизоров и панелей 70"-90"+ WizePro, усилитель-распределитель 1:4, передатчик PT-571, передатчик PT-572, масштабатор аналоговых и цифровых сигналов в сигналы HDMI с поддержкой аудио, PTZ-камера Prestel HD-PTZ412ST, универсальное крепление для камер, устройство записи и трансляции AREC SG-1, радиосистема с петличным микрофоном Shure, комплект кабелей и расходных аксессуаров, сетевой управляемый фильтр Energenie EG-PMS2-LAN, учебная доска.	
Лаборатория технологий и управления информационной безопасности	Специализированная мебель (место преподавателя, посадочные места для студентов) Материально-техническое оснащение: Автоматизированное рабочее место преподавателя (АРМ-П) в составе ПЭВМ, мультимедийного проектора, экрана – 1 комплект, 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, Система контроля и управления доступом, Система охранно-пожарной сигнализации, Система охранного видеонаблюдения, Сплит-система	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 (компьютерный класс библиотеки)	Материально-техническое оснащение: 17 компьютеров, объединенных в сеть, с выходом в Интернет и обеспечением доступа в электронную информационно-образовательную среду МИЭТ	Операционная система Microsoft Windows от 7 версии и выше, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Crome); Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-6.ОИБ «Способен соблюдать основные требования информационной безопасности при решении задач профессиональной деятельности» представлен отдельным документом и размещен 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 подкомпетенций и приобретения необходимых знаний, умений и навыков в рамках данного курса читаются лекции, проводятся практические занятия и лабораторные работы.

В процессе изучения курса предполагается самостоятельная работа студента при подготовке к лекционным, практическим занятиям, выполнению лабораторных и практических заданий, тестов, подготовке сообщений. При этом студент использует методические разработки, рекомендуемую литературу, библиотеку электронных модулей в электронной информационной образовательной среде ОРИОКС, Интернет-ресурсы, 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 студенту также необходимо предварительно ознакомиться с методическими указаниями, прочитать конспект лекций по данной тематике и соответствующие главы учебника (учебного пособия) и подготовить доклад по заданной тематике.

После теоретического рассмотрения материала преподаватель выдает каждому студенту практико-ориентированные **лабораторные работы** на применение рассмотренных материалов, которое студенты выполняют в рамках аудиторных занятий и 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. Консультации проводятся лектором еженедельно.

По завершению изучения дисциплины предусмотрен ***зачет с оценкой,*** 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 необходимых компетенций с методическими указаниями его выполнения и критериями оценки достижения формируемых

в дисциплине компетенций/подкомпетенций.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система, которая предполагает регулярную оценку приобретаемых знаний, умений и опыта деятельности студентов в накопленных баллах.

По сумме баллов, накопленных в течение семестра, выставляется итоговая оценка по дисциплине. Структура и график контрольных мероприятий доступен в ОРИОКС/ URL: http://orioks.miet.ru/

Мониторинг успеваемости студентов проводится в течение всего семестра.

Балы за посещаемость, выполнение и сдачу текущих заданий первый раз выставляются на 4-й неделе и затем корректируются на 8-й, 12-й, 17-й неделях в соответствии с порядком начисления баллов по дисциплине.

РАЗРАБОТЧИК:

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

Рабочая программа дисциплины «Основы информационной безопасности» по специальности 38.05.01 «Экономическая безопасность», специализации – «Управление экономической безопасностью» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры «10» января 2024 года, протокол №1.

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

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа согласована с кафедрой экономики, менеджмента и финансов
Заведующий кафедрой ЭМФ _____ /Г.П. Ермошина/

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 /