Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Обязательная**
№ дисциплины по учебному плану:	**Б1.О.18**
Трудоемкость в зачетных единицах:	**1 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**1 семестр - 32 часа;**
Практические занятия	**1 семестр - 64 часа;**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**1 семестр - 2 часа;**
Самостоятельная работа	**1 семестр - 81,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Тестирование**	
Промежуточная аттестация:	
Экзамен	**1 семестр - 0,5 часа;**

Москва 2026

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Потехецкий С.В. Идентификатор: R83b30a44-PotekhetskySV-31b213(	С.В. Потехецкий

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение основ знаний, определяющих квалификацию бакалавра по направлению подготовки «Информационная безопасность», а также формирование предметной области и понимания социальной значимости своей будущей профессии.

Задачи дисциплины

- изучение теоретических основ обеспечения информационной безопасности на предприятии (в организации), а также в областях теории информации и системного анализа;
- формирование готовности и способности к активной профессиональной деятельности в условиях информационного противоборства;
- приобретение навыков правильного оформления результатов учебной деятельности.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИД-2$_{ОПК-1}$ Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	знать: - национальные, межгосударственные и международные стандарты в области защиты информации.
ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ИД-1$_{ОПК-1.1}$ Разрабатывает порядок и правила применения программно-аппаратных средств защиты информации в компьютерных системах	знать: - нормативные правовые акты в области защиты информации. уметь: - классифицировать и оценивать угрозы безопасности информации.
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИД-1$_{ОПК-5}$ Использует основы правовых знаний в различных сферах деятельности	знать: - методы защиты информации от «утечки» по техническим каналам. уметь: - реализовывать правила разграничения доступа персонала к объектам доступа.
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики	ИД-1$_{ОПК-10}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к	знать: - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	обеспечению информационной безопасности объекта защиты	уметь: - применять нормативные документы по противодействию технической разведке.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность компьютерных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Основные составляющие информационной безопасности	14	1	4	-	4	-	-	-	-	-	6	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Основные составляющие информационной безопасности"
1.1	Вводная лекция	6		2	-	2	-	-	-	-	-	2	-	***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основные составляющие информационной безопасности" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основные составляющие информационной безопасности" ***Изучение материалов литературных источников:*** [1], 1-45 [2], 1-50 [3], 1-55 [4], 1-15
1.2	Основные положения системного подхода к обеспечению информационной безопасности	8		2	-	2	-	-	-	-	-	4	-	
2	Базовые основы защиты информации	130		28	-	60	-	-	-	-	-	42	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Базовые основы защиты информации" ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Базовые
2.1	Тема 3.Организационно-правовое и кадровое обеспечение системы информационной безопасности	24		4	-	12	-	-	-	-	-	8	-	

2.2	Тема 4. Финансово-экономическое обеспечение системы информационной безопасности	24		4	-	12	-	-	-	-	-	8	-	основы защиты информации" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Базовые основы защиты информации" ***<u>Изучение материалов литературных источников:</u>*** [1], 46-98 [2], 50-106 [3], 55-372 [4], 25-38
2.3	Тема 5. Инженерно-техническое обеспечение системы информационной безопасности	26		6	-	12	-	-	-	-	-	8	-	
2.4	Тема 6. Программно-аппаратное обеспечение системы информационной безопасности	26		6	-	12	-	-	-	-	-	8	-	
2.5	Тема 7. Аудит системы информационной безопасности	30		8	-	12	-	-	-	-	-	10	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**180.0**		**32**	**-**	**64**	**-**	**2**	**-**	**-**	**0.5**	**48**	**33.5**	
	Итого за семестр	**180.0**		**32**	**-**	**64**	**2**		**-**		**0.5**	**81.5**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Основные составляющие информационной безопасности

1.1. Вводная лекция

Организация учебного процесса на кафедре БИТ. Цель и содержание учебной дисциплины, характеристика ее составляющих; взаимосвязь учебной дисциплины с другими дисциплинами. Понятие информации и ее виды. Виды конфиденциальной информации. Угрозы безопасности информации. Каналы утечки информации.

1.2. Основные положения системного подхода к обеспечению информационной безопасности

Понятие концепции и политики информационной безопасности. Основные свойства системы. Применение системного подхода к анализу системы обеспечения информационной безопасности. Основы создания, функционирования и управления СОИБ на предприятии (в организации).

2. Базовые основы защиты информации

2.1. Тема 3.Организационно-правовое и кадровое обеспечение системы информационной безопасности

Силы и средства. Профессиональная этика.

2.2. Тема 4. Финансово-экономическое обеспечение системы информационной безопасности

Силы и средства. Определение затрат на обеспечение информационной безопасности. Анализ методов эффективности затрат на информационную безопасность.

2.3. Тема 5. Инженерно-техническое обеспечение системы информационной безопасности

Силы и средства. Классификация средств инженерно-технического обеспечения системы информационной безопасности. Подсистема инженерно-технической защиты территорий и помещений. Подсистема обнаружения и защиты технических каналов утечки информации. Средства обнаружения (поиска) технических каналов утечки информации.

2.4. Тема 6. Программно-аппаратное обеспечение системы информационной безопасности

Силы и средства. Программная защита информации. Средства программной защиты информации. Программно-аппаратная защита информации. Средства программно-аппаратной защиты информации..

2.5. Тема 7. Аудит системы информационной безопасности

Силы и средства. Технология проведения аудита информационной безопасности.

3.3. Темы практических занятий

1. Собеседование по теме «Организационно-правовое и кадровое обеспечение системы информационной безопасности;
2. Финансово-экономическое обеспечение системы информационной безопасности;
3. Затраты на обеспечение информационной безопасности;
4. Эффективность затрат на информационную безопасность;
5. Подсистема инженерно-технической защиты территорий и помещений;

6. Средства обнаружения и защиты технических каналов утечки информации;
7. Программно-аппаратное обеспечение системы информационной безопасности;
8. Программная защита информации;
9. Инженерно-техническое обеспечение системы информационной безопасности;
10. Угрозы безопасности информации. Каналы утечки информации;
11. Аудит системы информационной безопасности;
12. Средства защиты компьютерной информации от несанкционированного доступа и утечки по материально-вещественному каналу;
13. Конфиденциальная информация;
14. Основы создания, функционирования и управления системой обеспечения информационной безопасности;
15. Средства защиты информации на ПЭВМ;
16. Основы системы информационной безопасности;
17. Сущность информации;
18. Организационно-правовое обеспечение системы информационной безопасности;
19. Программно-аппаратная защита информации;
20. Кадровое обеспечение системы информационной безопасности.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Основные составляющие информационной безопасности"
2. Обсуждение материалов по кейсам раздела "Базовые основы защиты информации"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Базовые основы защиты информации"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)		Оценочное средство (тип и наименование)
		1	2	
Знать:				
национальные, межгосударственные и международные стандарты в области защиты информации	ИД-2$_{ОПК-1}$	+		Тестирование/Тест № 1; Тест № 2 Тестирование/Тест №6
нормативные правовые акты в области защиты информации	ИД-1$_{ОПК-1.1}$		+	Тестирование/Тест № 1; Тест № 2 Тестирование/Тест№3, №4
методы защиты информации от «утечки» по техническим каналам	ИД-1$_{ОПК-5}$		+	Тестирование/Тест № 1; Тест № 2 Тестирование/Тест№3, №4 Тестирование/Тест №5
руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	ИД-1$_{ОПК-10}$		+	Тестирование/Тест № 1; Тест № 2
Уметь:				
классифицировать и оценивать угрозы безопасности информации	ИД-1$_{ОПК-1.1}$		+	Тестирование/Тест№3, №4 Тестирование/Тест №5 Тестирование/Тест №6
реализовывать правила разграничения доступа персонала к объектам доступа	ИД-1$_{ОПК-5}$		+	Тестирование/Тест№3, №4 Тестирование/Тест №6
применять нормативные документы по противодействию технической разведке	ИД-1$_{ОПК-10}$		+	Тестирование/Тест № 1; Тест № 2

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

1 семестр

Форма реализации: Билеты (письменный опрос)

1. Тест №6 (Тестирование)

Форма реализации: Проверка задания

1. Тест № 1; Тест № 2 (Тестирование)
2. Тест №5 (Тестирование)
3. Тест№3, №4 (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №1)

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ», на основании семестровой и экзаменационной составляющих.

В диплом выставляется оценка за 1 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Агуреев, И. А. Инженерно-техническая защита информации. Ч. 3 : учебное пособие и лабораторный практикум для Инженерно-экономического института / И. А. Агуреев, А. Ю. Невский, С. С. Рыжиков, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ". – Москва : ВНИИгеосистем, 2021. – 98 с. – ISBN 978-5-8481-0250-5.;
2. Минзов, А. С. Управление рисками информационной безопасности : [монография] / А. С. Минзов, А. Ю. Невский, О. Р. Баронов ; ред. А. С. Минзов ; Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ). – Москва : ВНИИгеосистем, 2019. – 106 с. – ISBN 978-5-8481-0240-6.;
3. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ). – М. : Издательский дом МЭИ, 2009. – 372 с. – ISBN 978-5-383-00375-6.
http://elib.mpei.ru/elib/view.php?id=1468;
4. А. Б. Борисов- "Комментарий к Конституции Российской Федерации (постатейный): с комментариями Конституционного суда РФ", (5-е изд., перераб. и доп.), Издательство: "Книжный мир", Москва, 2013 - (256 с.)
https://biblioclub.ru/index.php?page=book&id=274620.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Видеоконференции (Майнд, Сберджаз, ВК и др);
5. Acrobat Reader;
6. 7-zip.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **Национальная электронная библиотека** - https://rusneb.ru/
6. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
7. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
8. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
9. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
10. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
11. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
12. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
13. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
14. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
15. **Официальный сайт Федеральной службы по надзору в сфере образования и науки** - https://obrnadzor
16. **Федеральный портал "Российское образование"** - http://www.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный

Учебные аудитории для проведения лабораторных занятий	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
Учебные аудитории для проведения промежуточной аттестации	М-509, Учебная лаборатория "Инженерно-техническая защита информации"	стол преподавателя, стул, стол письменный, мультимедийный проектор, экран, компьютер персональный, кондиционер, телевизор, стенд лабораторный
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Лекционная аудитория	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Основы информационной безопасности

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:
КМ-1 Тест № 1; Тест № 2 (Тестирование)
КМ-2 Тест№3, №4 (Тестирование)
КМ-3 Тест №5 (Тестирование)
КМ-4 Тест №6 (Тестирование)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Основные составляющие информационной безопасности					
1.1	Вводная лекция		+			+
1.2	Основные положения системного подхода к обеспечению информационной безопасности		+			+
2	Базовые основы защиты информации					
2.1	Тема 3.Организационно-правовое и кадровое обеспечение системы информационной безопасности		+	+	+	
2.2	Тема 4. Финансово-экономическое обеспечение системы информационной безопасности		+			
2.3	Тема 5. Инженерно-техническое обеспечение системы информационной безопасности			+	+	+
2.4	Тема 6. Программно-аппаратное обеспечение системы информационной безопасности			+		+
2.5	Тема 7. Аудит системы информационной безопасности		+			
Вес КМ, %:			20	20	35	25