

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:	Базовая
№ дисциплины по учебному плану:	Б1.Б.02
Трудоемкость в зачетных единицах:	1 семестр - 6;
Часов (всего) по учебному плану:	216 часов
Лекции	1 семестр - 32 часа;
Практические занятия	1 семестр - 48 часа;
Лабораторные работы	не предусмотрено учебным планом
Консультации	1 семестр - 2 часа;
Самостоятельная работа	1 семестр - 133,5 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 2020

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Потехецкий С.В.
	Идентификатор	R83b30a44-PotekhetskySV-31b213d

(подпись)

С.В. Потехецкий

(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель
образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка
подписи)

Заведующий выпускающей
кафедры

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю. Невский

(расшифровка
подписи)

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 способностью анализировать физические явления и процессы для решения профессиональных задач		знать: - анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты. уметь: - определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		знать: - физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты. уметь: - анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к обязательной части блока дисциплин 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 6 зачетных единиц, 216 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	41	1	8	-	13	-	-	-	-	-	20	-	<p><u>Подготовка к аудиторным занятиям:</u> Проработка лекции</p> <p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Основные составляющие информационной безопасности" подготовка к выполнению заданий на практических занятиях</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Основные составляющие информационной безопасности"</p> <p><u>Изучение материалов литературных источников:</u> [1], 1-205 [2], 1-272 [3], 1-287 [4], 1-324</p>
1.1	Вводная лекция	20		4	-	6	-	-	-	-	-	10	-	
1.2	Тема 2. Основы системы информационной безопасности	21		4	-	7	-	-	-	-	-	10	-	
2	Базовые основы защиты информации	139		24	-	35	-	-	-	-	-	80	-	
2.1	Тема 3. Организационно-правовое и кадровое обеспечение системы информационной безопасности	21	4	-	7	-	-	-	-	-	10	-		
2.2	Тема 4. Финансово-экономическое	20	3	-	7	-	-	-	-	-	10	-		

	обеспечение системы информационной безопасности												Повторение материала по разделу "Базовые основы защиты информации"
2.3	Тема 5. Инженерно-техническое обеспечение системы информационной безопасности	22	5	-	7	-	-	-	-	-	10	-	<u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы
2.4	Тема 6. Программно-аппаратное обеспечение системы информационной безопасности	33	6	-	7	-	-	-	-	-	20	-	<u>Подготовка домашнего задания:</u> Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Базовые основы защиты информации" материалу. Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам.
2.5	Тема 7. Аудит системы информационной безопасности	43	6	-	7	-	-	-	-	-	30	-	<u>Подготовка доклада, выступления:</u> Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: <u>Изучение материалов литературных источников:</u> [1], 1-205 [2], 1-272 [3], 1-287 [4], 1-324
	Экзамен	36.0	-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	216.0	32	-	48	-	2	-	-	0.5	100	33.5	
	Итого за семестр	216.0	32	-	48	2	-	-	-	0.5	133.5		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПП – 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 информации. Каналы утечки информации..

1.2. Тема 2. Основы системы информационной безопасности

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

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. Угрозы информации. Каналы утечки информации;
2. Основы системы информационной безопасности;
3. Контрольное мероприятие № 1;
4. Финансово-экономическое обеспечение системы информационной безопасности;
5. Затраты на обеспечение информационной безопасности;
6. Эффективность затрат на информационную безопасность;
7. Контрольное мероприятие № 2;

8. Инженерно-техническое обеспечение системы информационной безопасности;
9. Подсистема инженерно-технической защиты территорий и помещений;
10. Средства обнаружения и защиты технических каналов утечки информации;
11. Контрольное мероприятие № 3;
12. Программно-аппаратное обеспечение системы информационной безопасности;
13. Программная защита информации;
14. Средства защиты информации на ПЭВМ;
15. Программно-аппаратная защита информации;
16. Контрольное мероприятие № 4;
17. Аудит системы информационной безопасности;
18. Конфиденциальная информация;
19. Средства защиты компьютерной информации от несанкционированного доступа и утечки по материально-вещественному каналу;
20. Сущность информации.

3.4. Темы лабораторных работ не предусмотрено

3.5 Консультации

Текущий контроль (ТК)

1. Консультация по порядку проведения тестирования при выполнении контрольного мероприятия текущего контроля на 4 неделе
2. Консультация по порядку проведения тестирования и выполнения контрольного задания при выполнении контрольного мероприятия текущего контроля

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:				
анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	ОПК-1(Компетенция)	+		Тестирование/Тест №5 Тестирование/Тест №6
физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	ОПК-7(Компетенция)	+		Тестирование/Тест № 3; Тест № 4 Тестирование/Тест №5
Уметь:				
определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	ОПК-1(Компетенция)		+	Тестирование/Тест № 3; Тест № 4 Тестирование/Тест №5 Тестирование/Тест №6
анализировать физические явления и процессы, применяемые для обеспечения информационной безопасности объекта защиты	ОПК-7(Компетенция)	+	+	Тестирование/Тест № 1; Тест № 2 Тестирование/Тест № 3; Тест № 4

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 № 3; Тест № 4 (Тестирование)
2. Тест №5 (Тестирование)
3. Тест №6 (Тестирование)

Форма реализации: Проверка задания

1. Тест № 1; Тест № 2 (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 (экзамена, проводимого по билетам).

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Галатенко, В.А. Основы информационной безопасности : учебное пособие для вузов по специальности 351400 "Прикладная информатика" / В.А. Галатенко ; Ред. В. Б. Бетелин . – 4-е изд . – М. : Интернет-Ун-т информ. технологий : БИНОМ. Лаборатория знаний, 2010 . – 205 с. – (Основы информационных технологий) . - ISBN 978-5-94774-821-5 .;
2. Грушо, А. А. Теоретические основы компьютерной безопасности : учебное пособие для вузов по специальности 090100 "Информационная безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина . – М. : АКАДЕМИЯ, 2009 . – 272 с. – (Высшее профессиональное образование) . - ISBN 978-5-7695-4242-8 .;
3. В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев- "Основы информационной безопасности", Издательство: "Юнити-Дана|Закон и право", Москва, 2018 - (287 с.)
<https://biblioclub.ru/index.php?page=book&id=562348>;
4. Нестеров С. А.- "Основы информационной безопасности", (4-е изд., стер.), Издательство: "Лань", Санкт-Петербург, 2018 - (324 с.)
<https://e.lanbook.com/book/103908>.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office;
3. Windows;
4. Майнд Видеоконференции;
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 ВИНТИ online - <http://www.viniti.ru/>
5. Национальная электронная библиотека - <https://rusneb.ru/>
6. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
7. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
8. Портал открытых данных Российской Федерации - <https://data.gov.ru>
9. База открытых данных Министерства труда и социальной защиты РФ - <https://rosmintrud.ru/opendata>
10. База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ - <http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/>
11. База открытых данных Министерства экономического развития РФ - <http://www.economy.gov.ru>
12. База открытых данных Росфинмониторинга - <http://www.fedsfm.ru/opendata>
13. Электронная открытая база данных "Polpred.com Обзор СМИ" - <https://www.polpred.com>
14. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;>
<http://docs.cntd.ru/>
15. Национальный портал онлайн обучения «Открытое образование» - <https://openedu.ru>
16. Официальный сайт Федерального агентства по техническому регулированию и метрологии - <http://protect.gost.ru/>
17. Открытая университетская информационная система «РОССИЯ» - <https://uisrussia.msu.ru>
18. Официальный сайт Министерства науки и высшего образования Российской Федерации - <https://minobrnauki.gov.ru>
19. Официальный сайт Федеральной службы по надзору в сфере образования и науки - <https://obrnadzor>
20. 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 аудитория	парта со скамьей, стол преподавателя, стул, доска меловая
Учебные аудитории	М-509, Учебная	парта со скамьей, стол преподавателя,

для проведения промежуточной аттестации	аудитория	стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, 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

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; Тест № 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	Тема 2. Основы системы 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, %:			25	25	25	25