

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Беспалов Владимир Александрович

Должность: Ректор

Дата подписания: 01.09.2023 14:31:11

Уникальный программный ключ:

ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f736d76c8f8bea882b8d802

МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет

«Московский институт электронной техники»

УТВЕРЖДАЮ

Проректор по учебной работе

И.Г. Игнатова

«22» декабря 2020 г.

М.П.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки – **11.03.02 «Инфокоммуникационные технологии и системы связи»**

Направленность (профиль) – **«Сети и устройства инфокоммуникаций»**
«Сети и системы инфокоммуникаций»

Москва 2020

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

ОПК	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения компетенций
ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.ОИБ Способен соблюдать основные требования информационной безопасности при решении задач профессиональной деятельности.	<u>Знания:</u> - теоретических основ информационной безопасности. <u>Умения:</u> - применять методы и средства защиты информации. <u>Опыт:</u> - 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)		
2	4	3	108	24	-	24	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 и основные направления защиты информации	4	-	4	6	Контроль выполнения СРС к семинару 1.
					Тестирование 1.
2. Защита информации от несанкционированного доступа	8	-	2	30	Контроль выполнения СРС к семинару 2.
					Защита Домашних заданий 1-2.
					Тестирование 2.
3. Защита информации от утечки по техническим каналам	6	-	2	6	Контроль выполнения СРС к семинару 3.
					Тестирование 3.
4. Организация и управление информационной безопасностью	6	-	16	18	Защита Практических заданий 1-4.
					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	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.
	2.	2	Основные направления и задачи защиты информации Защита информации (определение). Основные направления 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		
	3.	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.
	4.	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
	5.	2	Методы и средства криптографической защиты информации Термины и определения в области криптографии. Классификация криптографических средств. Основные методы шифрования.
	6.	2	Методы и средства антивирусной защиты. Методы антивирусной защиты. Средства антивирусной защиты.
3	Защита информации от утечки по техническим каналам		
	7.	2	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.
	8.	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.
	9.	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		
	10.	2	Организация защиты информации Общий порядок организации защиты информации. Аналитическое обоснование необходимости создания системы защиты информации (СЗИ). Техническое задание на создание СЗИ
	11.	2	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
	12.	2	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	1-2	4	Практическое занятие (семинар №1). Средства и системы обработки данных.
2	3	2	Практическое занятие (семинар №2). Методы и средства защиты информации от несанкционированного доступа.
3	4	2	Практическое занятие (семинар №3). Методы и средства защиты информации от утечки по техническим каналам.
4	5-6	4	Практическое занятие (групповое упражнение №1). Разработка проекта «Концепции информационной безопасности коммерческой организации».
4	7-8	4	Практическое занятие (групповое упражнение №2). Разработка «Модели угроз безопасности информации для автоматизированной системы обработки конфиденциальной информации»
4	9-10	4	Практическое занятие (групповое упражнение №3). Разработка технического задания на создание системы защиты информации от несанкционированного доступа (на примере автоматизированной системы обработки конфиденциальной информации).
4	11-12	4	Практическое занятие (групповое упражнение №4). Разработка организационно-распорядительных документов по защите автоматизированной системы от несанкционированного доступа к информации.

4.3. Лабораторные занятия

Не предусмотрены

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	4	Подготовка к практическому занятию (семинар №1). Изучение материалов лекции №№1-2 и рекомендованной литературы. Изучение плана проведения семинара №1. Подготовка сообщения по одному из вопросов семинара
1	2	Подготовка к Тестированию 1. Изучение материалов лекции №№1-2 и рекомендованной литературы.
2	4	Подготовка к практическому занятию (семинар №2). Изучение материалов лекции №№3-6 и рекомендованной литературы. Изучение плана проведения семинара №2. Подготовка сообщения по одному из вопросов семинара
2	2	Подготовка к Тестированию 2. Изучение материалов лекции №№3-6 и рекомендованной литературы.
2	12	Домашнее задание 1. Установка и настройка средств защиты систем обработки данных на базе СВТ
2	12	Домашнее задание 2. Установка и настройка средств защиты. Функциональные требования безопасности
3	4	Подготовка к практическому занятию (семинар №3). Изучение материалов лекции №№7-9 и рекомендованной литературы. Изучение плана проведения семинара №3. Подготовка сообщения по одному из вопросов семинара
3	2	Подготовка к Тестированию 3. Изучение материалов лекции №№7-9 и рекомендованной литературы.
4	4	Подготовка к практическому занятию (групповое упражнение №1). Изучение материалов лекции №10-12 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения.
	4	Подготовка к практическому занятию (групповое упражнение №2) Изучение материалов лекции № 10-12 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения.
	4	Подготовка к практическому занятию (групповое упражнение №3) Изучение материалов лекции №10-12 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения.
	4	Подготовка к практическому занятию (групповое упражнение №4) Изучение материалов лекции № 10-12 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения.
	2	Подготовка к Тестированию 4. Изучение материалов лекции №№10-12 и рекомендованной литературы.
Итого	60	

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 и подготовки к выполнению практических заданий 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».

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Душкин А.В. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов; под ред. А.В. Душкина // М.: Горячая линия-Телеком, 2018. — 248 с. — URL: <https://e.lanbook.com/book/111053> (дата обращения: 21.11.2020).
2. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: справочник / Г.А. Бузов // М.: Горячая линия-Телеком, 2018. — 586 с. — URL: <https://e.lanbook.com/book/94625> (дата обращения: 21.11.2020).
3. Петренко В.И. Защита персональных данных в информационных системах. Практикум: учебное пособие / В.И. Петренко, И.В. Мандрица // СПб.: Лань, 2019. — 108 с. — URL: <https://e.lanbook.com/book/111916> (дата обращения: 21.11.2020).
4. Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков // М.: ДМК Пресс, 2017. — 434 с. — URL: <https://e.lanbook.com/book/93278> (дата обращения: 21.11.2020).
5. Малюк А.А. Защита информации в информационном обществе: учебное пособие / А.А. Малюк // М.: Горячая линия-Телеком, 2017. — 230 с. — URL: <https://e.lanbook.com/book/111078> (дата обращения: 21.11.2020).
6. Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации): учебное пособие / В.К. Новиков // М.: Горячая линия-Телеком, 2017. — 176 с. — URL: <https://e.lanbook.com/book/111084> (дата обращения: 21.11.2020).

Периодические издания

1. Специальная техника / ОАО "Электрозавод". - Москва : Электрозавод, 1998-2017. - В настоящее время не выходит; URL: <http://elibrary.ru/contents.asp?titleid=9851> (дата обращения: 21.11.2020). - 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: <http://elibrary.ru/contents.asp?titleid=25917> (дата обращения: 21.11.2020). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный
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: 21.11.2020). - 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: 05.07.2021). - Режим доступа: свободный. - ISSN 2311-3456. - Текст : электронный. Information Security / Информационная безопасность – URL: <http://www.itsec.ru/articles2/allpubliks> (дата обращения: 21.11.2020). – Режим доступа: свободный.

5. JET INFO : деловое издание. - Москва : Компания "Инфосистемы Джет", 1995 - . - URL: <http://www.jetinfo.ru/> (дата обращения: 21.11.2020). - Режим доступа: свободный. - Текст : электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Лань: Электронно-библиотечная система Издательства Лань. - СПб., 2011-. - URL: <https://e.lanbook.com> (дата обращения: 21.11.2020). - Режим доступа: для авторизованных пользователей МИЭТ.

2. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: <https://www.elibrary.ru/defaultx.asp> (дата обращения: 21.11.2020). - Режим доступа: для зарегистрированных пользователей.

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: 21.11.2020). - Режим доступа: свободный.

4. ФСБ России: Выписка из перечня средств защиты информации, сертифицированных ФСБ России – Москва, 2017 - URL: <http://www.fsb.ru/> (дата обращения: 21.11.2020). - 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, лабораторных работ, практических занятий, практико-ориентированных заданий, методических разработок по тематике курса и др., а также созданный преподавателем ресурс на Яндекс диске.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: раздел ОРИОКС «Домашние задания», 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	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-3.ОИБ Способен соблюдать основные требования информационной безопасности при решении задач профессиональной деятельности.

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: <http://orioks.miet.ru/>.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

Для формирования подкомпетенций и приобретения необходимых знаний, умений и навыков 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 сообщений и выполнению практико-ориентированных заданий. 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 (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 практическое домашнее задание на применение рассмотренных материалов, которое студенты выполняют в рамках СРС в течение заданного времени, получив на практическом занятии методические рекомендации по выполнению. 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 *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.

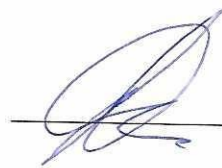
11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система.

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 направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи», направленности (профилю) – «Сети и устройства инфокоммуникаций», «Сети и системы инфокоммуникаций» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры «21» декабря 2020 года, протокол №12.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор

 / А.А. Хорев /

ЛИСТ СОГЛАСОВАНИЯ

Заведующий кафедрой
«Телекоммуникационные системы»

 / А.А. Бахтин /

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 /