

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Беспалов Владимир Александрович

Должность: Ректор МИЭТ

Дата подписания: 01.09.2025 12:28:16

Уникальный программный ключ:

ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f736

МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет

«Московский институт электронной техники»

УТВЕРЖДАЮ

Проректор по учебной работе

И.Г. Игнатова

« 9 » 12 202 0 г.

М.П.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки – 09.03.03 «Прикладная информатика»

Направленность (профиль) – «Системы корпоративного управления»

Форма обучения - заочная

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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.ИБ 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 (ЗЕТ)	Общая трудоёмкость (часы)	Контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
3	7	4	144	10	100	Э

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа	Самостоятельная работа	Формы текущего контроля
1. Угрозы безопасности информации и основные направления защиты информации	2	12	Контроль выполнения СРС 1.
			Тестирование 1.
2. Защита информации от несанкционированного доступа	2	38	Контроль выполнения СРС 2.
			Защита Домашних заданий 1-2.
			Тестирование 2
3. Защита информации от утечки по техническим каналам	2	12	Контроль выполнения СРС к семинару 3.
			Тестирование 3.
4. Организация и управление информационной безопасностью	4	38	Защита Практических заданий 1-4.
			Тестирование 4.

4.1. Самостоятельное изучение теоретического материала

№ модуля дисциплины	Объем работы (часы)	Краткое содержание
1	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.
	4	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	3	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.
	3	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.
	3	Методы и средства криптографической защиты информации Термины и определения в области криптографии. Классификация криптографических средств. Основные методы шифрования.
	3	Методы и средства антивирусной защиты. Методы антивирусной защиты. Средства антивирусной защиты.

№ модуля дисциплины	Объем работы (часы)	Краткое содержание
3	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.
	4	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.
	4	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	6	Организация защиты информации Общий порядок организации защиты информации. Аналитическое обоснование необходимости создания системы защиты информации (СЗИ). Техническое задание на создание СЗИ
	6	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.
	8	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	Объем работы (часы)	Наименование задания
1	4	Средства и системы обработки данных.
2	2	Методы и средства защиты информации от несанкционированного доступа.
3	2	Методы и средства защиты информации от утечки по техническим каналам.
4	4	Разработка проекта «Концепции информационной безопасности коммерческой организации».
4	4	Разработка «Модели угроз безопасности информации для автоматизированной системы обработки конфиденциальной информации»
4	4	Разработка технического задания на создание системы защиты информации от несанкционированного доступа (на примере автоматизированной системы обработки конфиденциальной информации).
4	4	Разработка организационно-распорядительных документов по защите автоматизированной системы от несанкционированного доступа к информации.

4.3. Дополнительные виды самостоятельной работы

№ модуля дисциплины	Объем работы(часы)	Вид СРС
1	2	Подготовка к Тестированию 1.
2	2	Подготовка к Тестированию 2..
2	12	Домашнее задание 1. Установка и настройка средств защиты АС на базе АРМ с использованием возможностей ОС Windows. Установка и настройка средств антивирусной защиты
2	12	Домашнее задание 2. Установка и настройка средств межсетевого экранирования
3	2	Подготовка к Тестированию 3.
4	2	Подготовка к Тестированию 4. Изучение материалов лекции №№10-12 и рекомендованной литературы.

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». — URL: <http://ess.ru/index.htm> (дата обращения: 21.11.2020). — Режим доступа: свободный.
2. «Защита информации. Инсайд». — URL: <http://www.inside-zi.ru> (дата обращения: 21.11.2020). — Режим доступа: свободный.
3. «Безопасность информационных технологий». — URL: http://www.pvti.ru/articles_14.htm (дата обращения: 21.11.2020). — Режим доступа: свободный.
4. «Информация и безопасность». — URL: http://kafedrasib.ru/?page_id=119 (дата обращения: 21.11.2020). — Режим доступа: свободный.

5. «Безопасность информационных технологий». – URL: <https://bit.mephi.ru/index.php/bit> (дата обращения: 21.11.2020). – Режим доступа: свободный.

6. «Вопросы кибербезопасности». – URL: <http://cyberrus.com/> (дата обращения: 21.11.2020). – Режим доступа: свободный.

7. «Information Security / Информационная безопасность». – URL: <http://www.itsec.ru/articles2/allpubliks> (дата обращения: 21.11.2020). – Режим доступа: свободный.

8. Информационный бюллетень «Jet Info». «Инфосистемы Джет». – URL: <http://www.jetinfo.ru> (дата обращения: 21.11.2020). – Режим доступа: свободный.

9. Бюро научно-технической информации «Техника для спецслужб». – URL: <http://www.bnti.ru/about.asp> (дата обращения: 21.11.2020). – Режим доступа: свободный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Электронно-библиотечная система «ЭБС ЮРАЙТ». – <https://www.biblio-online.ru> (дата обращения: 21.11.2020). – Режим доступа: для авториз. пользователей МИЭТ.

2. Электронно-библиотечная система «BOOK.ru». – <https://www.book.ru> (дата обращения: 21.11.2020). – Режим доступа: для авториз. пользователей МИЭТ.

3. Электронно-библиотечная система ЛАНЬ. – <http://www.e.lanbook.com> (дата обращения: 21.11.2020). – Режим доступа: для авториз. пользователей МИЭТ.

4. Электронно-библиотечная система «ZNANIUM.COM». – <http://www.znanium.com> (дата обращения: 21.11.2020). – Режим доступа: для авториз. пользователей МИЭТ.

5. Электронно-библиотечная система eLIBRARY. – <http://www.elibrary.ru> (дата обращения: 21.11.2020). – Режим доступа: для авториз. пользователей МИЭТ.

6. Научометрическая база данных Scopus. – <http://www.scopus.com/> (дата обращения: 21.11.2020). – Режим доступа: для авториз. пользователей МИЭТ.

7. Научометрическая база данных Web of Science. – <http://apps.webofknowledge.com> (дата обращения: 21.11.2020). – Режим доступа: для авториз. пользователей МИЭТ.

8. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). – <https://fstec.ru/> (дата обращения: 21.11.2020). – Режим доступа: свободный.

9. Сайт Федеральной службы безопасности России (ФСБ России). – <http://www.fsb.ru/> (дата обращения: 21.11.2020). – Режим доступа: свободный.

10. Портал технического комитета по стандартизации «Защита информации». – <http://tk.gost.ru/wps/portal/tk362> (дата обращения: 21.11.2020). – Режим доступа: свободный.

11. Информационно-аналитический Интернет-портал ISO27000.ru. – <http://www.iso27000.ru> (дата обращения: 21.11.2020). – Режим доступа: свободный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Обучение реализуется с применением электронного обучения и дистанционных

образовательных технологий.

В процессе обучения 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.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для изучения дисциплины студенту необходима компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ.

Необходимое программное обеспечение: операционная система Microsoft Windows; пакет программ MS Office; браузер Google Chrome.

Антивирус Касперского, DrWeb, EsetNod32, Microsoft Security Essentials, Avast, Oracle VM VirtualBox, , Mware Player, Cisco_Packet_Tracer.

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-3.ИБ 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 студенту необходимо изучить теоретический материал и выполнить практические задания..

Особенность обучения с использованием электронного обучения, дистанционных образовательных технологий заключается в самостоятельном освоении дисциплины. В соответствии с графиком обучения, выданным перед началом обучения и имеющимся в ОРИОКС, выполняйте все учебные мероприятия.

В процессе изучения курса преподавателем проводятся консультационные занятия, обсуждение результатов выполнения контрольных мероприятий. На консультациях студентам даются пояснения по трудноусваиваемым разделам дисциплины. Задать вопрос преподавателю можно по электронной почте или в ZOOM.

Промежуточная аттестация может проходить как с использованием дистанционных

образовательных технологий, так и очно.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме до 100 баллов).

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

РАЗРАБОТЧИК:

Доцент СПИНТех
К.т.н., доцент

 / Н.Ю.Соколова /

Рабочая программа дисциплины «Информационная безопасность» по направлению подготовки 09.03.03 «Прикладная информатика», направленности (профилю)– «Системы корпоративного управления» разработана в Институте СПИНТех и утверждена на заседании кафедры «24» ноября 2020 года, протокол №3.

Директор Института системной и программной инженерии
и информационных технологий _____ / Л.Г. Гагарина /

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 /