

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Беспалов Владимир Александрович

Должность: Ректор МИЭТ

Дата подписания: 01.09.2023 14:16:26

Уникальный программный ключ:

ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f7367ac893de4821b8d802

МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет

«Московский институт электронной техники»



УТВЕРЖДАЮ

Проректор по учебной работе

И.Г. Игнатова

«24» июля 2020 г.

* М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление – 11.03.01 Радиотехника

Направленность (профиль) – «Проектирование радиоинформационных систем»

Москва 2020

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

Компетенция	Подкомпетенции, формируемые для дисциплины	Индикаторы достижения подкомпетенций
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.ИБ Способен соблюдать требования информационной безопасности при поиске, хранении, обработке, анализе и представлении в требуемом формате информации из различных источников и баз данных	Знания: этапов и методологии применения аппаратно-программных систем информационной безопасности Умения: интерпретировать результаты анализа проблем информационной безопасности объекта информатизации в соответствии с поставленной задачей Опыт: деятельности –оценка состояния информационной безопасности объектов информатизации и эффективности применения средств аппаратно-программной защиты

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы.

Для освоения дисциплины должны быть изучены следующие дисциплины или модули образовательной программы: «Специальные разделы мат. анализа» (модули «Теория функций комплексного переменного», «Преобразование Фурье»), «Дифференциальные уравнения», «Математический анализ», «Дискретная математика», «Электротехника», «Электроника и импульсная техника».

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)		
3	6	3	108	32	-	16	60	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные занятия (часы)	Практические занятия (часы)		
Модуль 1. Комплексная защита	8	-	4	15	Контрольные работы Проверка выполнения индивидуального самостоятельного задания
Модуль 2. Деструктивные воздействия	8	-	4	15	Контрольные работы Проверка выполнения индивидуального самостоятельного задания
Модуль 3. Средства защиты	8	-	4	15	Контрольные работы Проверка выполнения индивидуального самостоятельного задания
Модуль 4. Современные комплексные системы защиты	8	-	4	15	Контрольные работы Проверка выполнения индивидуального самостоятельного задания

4.1. Лекционные занятия

№ модуля	дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1		1	2	Предмет и задачи защиты информации. Особенности аппаратной защиты. Комплексный подход к проблеме защиты информации. Идентификация субъекта. Защита компьютеров и компьютерных сетей. Протокол идентификации. Электронная цифровая подпись. Роль аппаратной защиты.
		2	2	Построение аппаратных компонент криптозащиты данных. Необходимые и достаточные функции аппаратного средства криптозащиты. Аппаратное шифрование. Принцип чувствительной области и принцип главного ключа. Полностью контролируемые компьютерные системы. Программная реализация функций и защита программ аппаратными методами. Аппаратная реализация функций. Частично контролируемые компьютерные системы. Контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам.
		3	2	Технические каналы утечки информации. Утечка информации по акустическим каналам. Акустические каналы. Технические средства для съема информации по акустическим каналам. Противодействие утечке аудиоинформации. Акустическая защита речи.
		4	2	Прослушивание телефонных переговоров. Методы защиты информации, передающейся по телефонным линиям связи. Скремблирование. Типы скремблеров. Закрывание речевых сигналов в ТЛС. Нелинейные локаторы.
2		5	2	Силовые деструктивные воздействия на информационные системы. Защита от деструктивного воздействия на информационные системы. Современные технические средства силового разрушающего или поражающего воздействия. Критерии качества функционирования технических средств защиты.
		6	2	Деструктивные воздействия на компьютерные системы по цепям электропитания. Защита от деструктивного воздействия по цепям электропитания. Классификация технических средств силового деструктивного воздействия по сетям питания. Варианты питания компьютеров от сети. Технические характеристики сетевых фильтров. Устройства бесперебойного питания.
		7	2	Технические средства силового деструктивного воздействия по проводным каналам. Защита от деструктивного воздействия по проводным линиям связи. Классификация технических средств силового деструктивного воздействия по проводным каналам связи. Организационные и технические мероприятия, необходимые для

			защиты информационных систем от силового деструктивного воздействия по проводным линиям связи
	8	2	Беспроводные технические средства силового деструктивного воздействия. Защита от деструктивного воздействия по эфиру. Классификация беспроводных технических средств силового деструктивного воздействия. Организационные и технические мероприятия по защите информационных систем от беспроводных средств силового деструктивного воздействия. Экранирование и заземление как основные методы защиты от беспроводных средств силового деструктивного воздействия.
3	9	2	Современные аппаратно-программные средства аутентификации. Электронные ключи. Программный компонент электронного ключа. Защитный конверт. Библиотечные функции обращения к ключу API. Типы электронных ключей. Ключи HASP. Смарт-карты. Электронные жетоны. Программно-аппаратные комплексы защиты. Идентифицирующая информация.
	10	2	Биометрические средства защиты. Особенности биометрических средств. Системы идентификации, анализирующие характерные черты личности человека. Показатели надежности биометрических средств. Типовой состав биометрической системы защиты.
	11	2	Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды. Постановка задачи борьбы с разрушающими программными воздействиями. Формализация начальных условий задачи. Общие методы защиты программного обеспечения, решающие задачи борьбы со случайными сбоями оборудования и несанкционированным доступом. Специальные методы выявления программ с потенциально опасными последствиями. Формулировка необходимых и достаточных условий недопущения разрушающего воздействия. Изолированная программная среда.
	12	2	Защита программ от несанкционированного копирования. Технические средства защиты программ. Системы защиты персональных данных. Защита файлов от изменения. Ключи защиты программ. Организация хранения ключей. Проблемы защиты и взлома программ. Защита программ от изучения, защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям. Пример системы технической защиты. Методы нейтрализации защиты. Примеры систем защиты персональных данных.
4	13	2	Построение сложных аппаратно-программных систем защиты. Цифровая мобильная связь стандарта GSM. Проблемы защиты данных мобильной связи стандарта GSM. Общие характеристики стандарта GSM. Структурная схема и состав оборудования сетей связи. Сетевые и радио-интерфейсы. Структура служб и передача данных в стандарте GSM. Проблемы безопасности в цифровой сотовой системе связи GSM.
	14	2	Теоретические принципы построения систем передачи данных на основе шумоподобных сигналов (ШПС). Анализ ШПС систем с точки

			зрения информационной безопасности. Системы передачи данных с расширением спектра прямой последовательностью. Системы связи на базе ШПС. Оценка защищенности систем с кодированием прямой последовательностью. Системы множественного доступа на основе кодирования прямой последовательностью и информационная безопасность.
	15	2	Цифровая мобильная связь стандарта CDMA. Преимущества систем связи, использующих расширение спектра сигнала. Проблемы безопасности мобильной связи и пути их решения. Основные принципы функционирования стандарта CDMA. Стандарт CDMA IS-95. Отличие CDMA IS-95 от других сетей мобильной связи. Услуги в сетях CDMA IS-95, технология мультимедиа. Развитие и перспективы CDMA в будущем. Сети третьего поколения. Возможность несанкционированного (двойного) подключения в сети CDMA. Технология A-Key. Решение проблем безопасности в цифровой сотовой системе связи CDMA.
	16	2	Сети мобильной широкополосной связи типа Wi-Fi. Проблема аппаратно-программной защиты широкополосных сетей. Беспроводные локальные сети. Стандарты семейства протоколов IEEE 802.11. Развитие сетей WLAN за рубежом. Подход к информационной безопасности. WLAN в России. Оценка проблемы защиты данных.

4.2. Практические занятия

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Краткое содержание
1	1	4	Аппаратная реализация алгоритмов шифрования
2	2	4	Аппаратная реализация алгоритмов аутентификации
3	3	4	Аутентификация и идентификация
4	4	4	Аппаратная реализация комплексной защиты вычислительной системы

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	5	Самостоятельное изучение дополнительной литературы и электронных

		ресурсов по темам лекций
	6	Самостоятельная работа по подготовке к контрольным работам
	4	Выполнение индивидуального самостоятельного задания по тематикам практических занятий
2	5	Самостоятельное изучение дополнительной литературы и электронных ресурсов по темам лекций
	6	Самостоятельная работа по подготовке к контрольным работам
	4	Выполнение индивидуального самостоятельного задания по тематикам практических занятий
3	5	Самостоятельное изучение дополнительной литературы и электронных ресурсов по темам лекций
	6	Самостоятельная работа по подготовке к контрольным работам
	4	Выполнение индивидуального самостоятельного задания по тематикам практических занятий
4	5	Самостоятельное изучение дополнительной литературы и электронных ресурсов по темам лекций
	6	Самостоятельная работа по подготовке к контрольным работам
	4	Выполнение индивидуального самостоятельного задания по тематикам практических занятий

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, <http://orioks.miet.ru/>):

- Методические указания студентам по изучению дисциплины
- Презентационный материал к лекциям,
- Методические указания по выполнению домашних заданий по курсу
- Материалы для выполнения практико-ориентированного задания:

СРС: варианты заданий, примеры выполнения заданий

контрольных/самостоятельных работ

СРС: варианты заданий для дифференцированного зачета

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

1. Хорев П.Б. Программно-аппаратная защита информации : Учеб. пособие / П.Б. Хорев. - М. : Форум, 2013. - 352 с. - (Высшее образование). - ISBN 978-5-91134-353-8 : 352-00, 1500 экз.
2. Авторы: Хорев П.Б. Шаньгин, В. Ф. (Автор МИЭТ, ИПОВС). Информационная безопасность и защита информации : [учебное пособие] / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2014. - 702 с. - URL: <https://e.lanbook.com/book/50578> (дата обращения: 06.10.2020). - ISBN 978-5-94074-768-0. - Текст : электронный.
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. - Москва : Юрайт, 2020. - 312 с. - (Высшее образование). - URL: <https://urait.ru/bcode/452368> (дата обращения: 09.10.2020). - ISBN 978-5-9916-9043-0. - Текст : электронный.
4. Малюк, А. А. Защита информации в информационном обществе / А. А. Малюк. - Москва : Горячая линия-Телеком, 2017. - 230 с. - URL: <https://e.lanbook.com/book/111078> (дата обращения: 30.10.2020). - ISBN 978-5-9912-0481-1. - Текст : электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. IEEE/IET Electronic Library (IEL) [Электронный ресурс] = IEEE Xplore : Электронная библиотека. - USA ; UK, 1998-. - URL: <https://ieeexplore.ieee.org/Xplore/home.jsp> (дата обращения : 28.10.2020). - Режим доступа: из локальной сети НИУ МИЭТ в рамках проекта «Национальная подписка»
2. Лань : Электронно-библиотечная система Издательства Лань. - СПб., 2011-. - URL: <https://e.lanbook.com> (дата обращения: 28.10.2020). - Режим доступа: для авторизованных пользователей МИЭТ
3. Юрайт : Электронно-библиотечная система : образовательная платформа. - Москва, 2013 - . - URL: <https://urait.ru/> (дата обращения : 05.11.2020); Режим доступа: для авторизованных пользователей МИЭТ.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации дисциплины используется **смешанное обучение**, в основе которого лежит интеграция технологий традиционного и электронного освоения компетенций, в частности за счет использования таких инструментов как видео-лекции, онлайн тестирование, взаимодействие со студентами в электронной образовательной среде.

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

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: раздел ОРИОКС «Домашние задания», электронная почта, сервисы видеоконференцсвязи и социальные сети.

В процессе обучения при проведении занятий и для самостоятельной работы используются **внутренние электронные ресурсы** в формах тестирования в ОРИОКС и MOODLe.

При проведении занятий и для самостоятельной работы используются **внешние электронные ресурсы** в формах электронных компонентов видео-сервисов:

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень программного обеспечения
Учебная аудитория	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ Телевизор LG 55LV70S	Win pro от 7, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Chrome); Acrobat reader DC
Лаборатория прототипирования и тестирования ИУС	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Panasonic PT-LW373 HP ProCurve Switch 2848 J4904A HP ProCurve Switch 2824 J4904A National Instruments ELVIS National Instruments NI PXI-1033	Win pro от 7, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Chrome); Acrobat reader DC
Помещение для самостоятельной работы	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ	Win pro от 7, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Chrome); Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ ФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-3.ИБ «Способность соблюдать требования информационной безопасности при поиске, хранении, обработке, анализе и представлении в требуемом формате информации из различных источников и баз данных».

Фонд оценочных средств представлен отдельным документом и размещен в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: <https://orioks.miet.ru/>

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

«Информационная безопасность» основана на законах дискретной математики. Поэтому студенты должны освоить соответствующую дисциплину для успешного усвоения материала по данному курсу.

Знание основ информационной безопасности в настоящее время нужно рассматривать как вопрос грамотности любого технического специалиста. Основы информационной безопасности нетрудно понять и освоить, так как суть их проста, а число важных принципов невелико. Конкретная же реализация защиты, которая может быть спроектирована на их основе, имеет безграничное число вариантов.

В настоящем курсе «Информационная безопасность» материал представлен четырьмя модулями. В каждом из них даются знания о конкретной области защиты.

Все модули могут быть изучены как логически-законченные темы с собственными индивидуальными заданиями на лабораторных работах.

Для закрепления полученных знаний и в качестве практической составляющей подготовки студентов, ими выполняются самостоятельные работы по тематике практических занятий (или семинарных, не знаю что лучше). Самостоятельные работы могут проходить как аудиторно (в аудитории для самостоятельной подготовки), так и дома. Самостоятельные работы включают в себя использование практических навыков при расчете данных, полученных в ходе решения задач, но без помощи преподавателя и выполняются каждым студентом индивидуально.

По завершению обучения проводится представление результатов выполнения самостоятельного задания, оно может проводиться как на лабораторных работах, так и дистанционно (путем общения с преподавателем по средствам электронной связи).

Критерием оценки самостоятельных работ является совокупность данных, реализованных и продемонстрированных в каждом конкретном случае.

Полученные знания, используются студентами при выполнении индивидуального задания, а также при написании выпускных квалификационных работ. Опыт, полученный студентами при выполнении лабораторных работ, несомненно, пригодится при работе по специальности.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется балльная накопительная система.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме 56 баллов максимально), активность в семестре (в сумме 4 баллов максимально) и сдача экзамена (40 баллов максимально).

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

РАЗРАБОТЧИК:

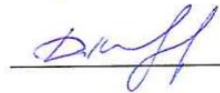
Доцент Института МПСУ, к.т.н.



/ Н.В. Степанов /

Рабочая программа дисциплины «Информационная безопасность» по направлению подготовки 11.03.01 Радиотехника, направленности (профиля) «Проектирование радиоинформационных систем» разработана в Институте МПСУ и утверждена на заседании ученого совета Института МПСУ «30» октября 2020 года, протокол № 1

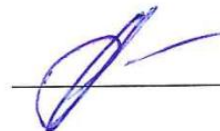
Зам. директора Института МПСУ

 /Д.В. Калеев/

ЛИСТ СОГЛАСОВАНИЯ

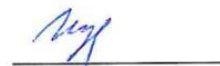
Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества.

Начальник АНОК

 /И.М. Никулина /

Рабочая программа согласована с библиотекой МИЭТ.

/Директор библиотеки

 /Т.П. Филиппова /