МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.Г. Балашов
«__» _____ 2023 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Защита информации»

Направление подготовки – 09.03.01 «Информатика и вычислительная техника»
Направленность (профиль) – «Программно-аппаратное обеспечение вычислительных систем» (очно-заочная форма обучения)

Москва 2023 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

Компетенция ПК-3 Способен управлять безопасностью сетевых устройств и программного обеспечения сформулирована на основе профессионального стандарта 06.027 Специалист по администрированию сетевых устройств информационно-коммуникационных систем

Обобщенная трудовая функция D – Администрирование процесса управление, безопасностью сетевых устройств и программного обеспечения.

Трудовая функция D/03.6 Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-3.ЗИ Способен решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	Поиск и диагностика ошибок сетевых устройств и программного обеспечения	**Знания** принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности в части защиты информации **Умения** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности в части защиты информации **Опыт** владения навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности в части защиты информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» образовательной программы.

Для освоения дисциплины должны быть изучены следующие дисциплины или модули образовательной программы: «Дифференциальные уравнения», «Математический анализ», «Дискретная математика», «Основы электротехники и схемотехники».

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	5	180	16	16	16	96	Экз (36)

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	4	4	4	24	Защита лабораторных работы Выполнение контрольной работы Сдача индивидуального задания Входное тестирование
Модуль 2. Деструктивные воздействия	4	4	4	24	Защита лабораторных работы Выполнение контрольной работы Сдача индивидуального задания

Модуль 3. Средства защиты	4	4	4	24	Защита лабораторных работы Выполнение контрольной работы Сдача индивидуального задания
Модуль 4. Современные комплексные системы защиты	4	4	4	24	Защита лабораторных работы Выполнение контрольной работы Сдача индивидуального задания

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1	2	Предмет и задачи защиты информации. Особенности аппаратурной защиты. Комплексный подход к проблеме защиты информации. Идентификация субъекта. Защита компьютеров и компьютерных сетей. Протокол идентификации. Электронная цифровая подпись. Роль аппаратной защиты. 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.
	2	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. Прослушивание телефонных переговоров. Методы защиты информации, передающейся по телефонным линиям связи. Скремблирование. Типы скремблеров. Закрытие речевых сигналов в ТЛС. Нелинейные локаторы.

2	3	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. 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.
	4	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 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	5	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. Биометрические средства защиты. Особенности биометрических средств. Системы идентификации, анализирующие характерные черты личности человека. Показатели надежности биометрических средств. Типовой состав биометрической системы защиты.

	6	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. 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	7	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. 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.
	8	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 мультидоступа. 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. 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

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Краткое содержание
1	1	4	Защита компьютера вне сети
2	2	4	Защита компьютера в сети
3	3	4	Оценка надежности защиты компьютера и средства ее повышения
4	4	4	Аппаратная реализация на базе среды LabViewNI комплексной системы защиты вычислительной системы

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	4	Самостоятельное изучение дополнительной литературы и электронных ресурсов сети интернет по темам лекций
	8	Самостоятельная работа по подготовке к контрольным работам
	8	Самостоятельная работа по подготовке к лабораторным работам
	4	Выполнение индивидуального задания
2	4	Самостоятельное изучение дополнительной литературы и электронных ресурсов сети интернет по темам лекций
	8	Самостоятельная работа по подготовке к контрольным работам
	8	Самостоятельная работа по подготовке к лабораторным работам
	4	Выполнение индивидуального задания
3	4	Самостоятельное изучение дополнительной литературы и электронных ресурсов сети интернет по темам лекций
	8	Самостоятельная работа по подготовке к контрольным работам

	8	Самостоятельная работа по подготовке к лабораторным работам
	4	Выполнение индивидуального задания
4	4	Самостоятельное изучение дополнительной литературы и электронных ресурсов сети интернет по темам лекций
	8	Самостоятельная работа по подготовке к контрольной работе по шумоподобным сигналам
	8	Самостоятельная работа по подготовке к лабораторной работе по аппаратной реализации на базе ПЛИС комплексной системы защиты вычислительной системы
	4	Выполнение индивидуального задания

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: https://orioks.miet.ru/):

- ✓ Сценарий к дисциплине;
- ✓ Методические рекомендации по выполнению лабораторных работ;
- ✓ Ссылки на литературу по всей дисциплине;
- ✓ Варианты контрольных вопросов для экзамена.

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

1. 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: 10.10.2023). - ISBN 978-5-94074-768-0. - Текст : электронный.
2. 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: 10.10.2023). - ISBN 978-5-9916-9043-0. - Текст : электронный.
3. 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.
4. Малюк А.А.Теория защиты информации / А.А. Малюк. - М. : Горячая линия-Телеком, 2012. - 184 с. - URL: https://e.lanbook.com/book/5170 (дата обращения: 10.10.2023). - ISBN 978-5-9912-0246-6.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. IEEE/IET Electronic Library (IEL) = IEEE Xplore : Электронная библиотека. - USA ; UK, 1998-. - URL: https://ieeexplore.ieee.org/Xplore/home.jsp (дата обращения : 10.10.2023).

- 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: 10.10.2023). - Режим доступа: для авторизированных 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 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:

корпоративная информационно-технологическая платформа ОРИОКС (http://orioks.miet.ru).

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	Компьютер с мультимедийным оборудованием	Win pro от 7, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Chrome); Acrobat reader DC
Лаборатория аппаратных и программных средств ИУС	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду HP ProCurve Switch 2824 J4903A ZyXEL omni LAN Switch G8 EE	Win pro от 7, Microsoft Office Professional Plus или Open Office, браузер (Firefox, Google Chrome); 7z Acrobat Reader DC Cisco packet tracer

	ZyXEL omni LAN Switch G8 EE Epson EB-G5600	
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 **ПК-3.ЗИ «**Способен решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности».

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

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

Знание основ защиты информации в настоящее время нужно рассматривать как вопрос грамотности любого технического специалиста. Основы защиты информации 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 «Защита информации» 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.

Рекомендуется перед выполнением лабораторной работы ознакомиться с заданием и ходом ее выполнения.

В процессе выполнения работы преподаватель помогает студентам, отвечая на их вопросы. Прежде, чем обратиться за помощью преподавателя, рекомендуется предварительно сформировать собственное мнение по интересующему вопросу, и, при необходимости, корректировать его, выслушав советы преподавателя.

Защита лабораторной работы проводится в процессе выполнения последующей лабораторной работы в интервал времени, который студент считает целесообразным выделить для этих целей.

Для закрепления полученных знаний и в качестве практической составляющей подготовки студентов, ими выполняются самостоятельные работы по тематике лабораторных работ. Самостоятельные работы могут проходить как аудиторно (в аудитории для самостоятельной подготовки), так и дома. Самостоятельные работы включают в себя использование практических навыков при модификации программного кода, написанного на лабораторных работах, но без помощи преподавателя и выполняются каждым студентом индивидуально.

Критериями оценки самостоятельных работ являются корректность полученных результатов, обоснованность выбранных подходов, своевременность сдачи заданий.

Полученные знания на лекциях, а также на лабораторных работах, 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/.

РАЗРАБОТЧИКИ:

Старший преподаватель Института МПСУ  А.И. Шариков

Рабочая программа дисциплины «Защита информации» по направлению подготовки 09.03.01 «Информатика и вычислительная техника», направленности (профиля) «Программно-аппаратное обеспечение вычислительных систем» (очно-заочная форма обучения) разработана в Институте МПСУ и утверждена на заседании ученого совета Института МПСУ «25» октября 2023 г., протокол №1.

Директор Института МПСУ _____/ А.Л. Переверзев /

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 /