

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Котова Лариса Анатольевна
Должность: Директор филиала
Дата подписания: 17.08.2024 12:14:01
Уникальный программный ключ:
10730ffe6b1ed036b744b6e9d97700b86e5c04a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский технологический университет «МИСИС»
Новотроицкий филиал

Аннотация рабочей программы дисциплины

Интеллектуальные технологии в металлургии

Закреплена за подразделением Кафедра математики и естествознания (Новотроицкий филиал)

Направление подготовки 09.03.03 Прикладная информатика

Профиль Прикладная информатика в технических системах

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе: Формы контроля в семестрах:
зачет с оценкой 7
аудиторные занятия 68
самостоятельная работа 76

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	19			
Неделя	УП	РП	УП	РП
Лекции	34	34	34	34
Лабораторные	17	17	17	17
Практические	17	17	17	17
Итого ауд.	68	68	68	68
Контактная работа	68	68	68	68
Сам. работа	76	76	76	76
Итого	144	144	144	144

1. ЦЕЛИ ОСВОЕНИЯ

1.1	Цели освоения дисциплины: понимание моделей и стандартов информационной безопасности, усвоение методов защиты информационных систем, приобретение теоретических знаний и практических навыков по использованию современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.
1.2	
1.3	Задачи:
1.4	- изучить основные теоретические положения защиты информации, причины нарушений безопасности;
1.5	- получить практические навыки работы с современными сетевыми фильтрами и средствами криптографического преобразования информации.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Блок ОП:		Б1.В.ДВ.03
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	Средства информатизации в металлургии	
2.1.2	Средства информатизации в энергетике	
2.1.3	Вычислительные системы, сети и телекоммуникации	
2.1.4	Языки программирования	
2.1.5	Компьютерная графика	
2.1.6	Архитектура ЭВМ и систем	
2.1.7	Информатика	
2.1.8	CASE-технологии	
2.1.9	Программная инженерия	
2.1.10	Учебная практика по получению первичных профессиональных умений	
2.1.11	Информационные системы и технологии	
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Информационная безопасность	
2.2.2	Основы микропроцессорной техники	
2.2.3	Подготовка к процедуре защиты и защита выпускной квалификационной работы	
2.2.4	Преддипломная практика	
2.2.5	Цифровые двойники в металлургии	

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ

ПК-1: Способен выполнять работы по критическому анализу функционирования технических систем, выявлять объекты информатизации и осуществлять работу по созданию или совершенствованию информационной системы	
Знать:	
ПК-1-31 применять методы проектирования прикладных технологий и систем	
ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	
Знать:	
ОПК-2-31 методы математического анализа и моделирования,	
ПК-1: Способен выполнять работы по критическому анализу функционирования технических систем, выявлять объекты информатизации и осуществлять работу по созданию или совершенствованию информационной системы	
Уметь:	
ПК-1-У1 методами проектирования прикладных технологий и систем	
ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	
Уметь:	
ОПК-2-У1 применять методы проектирования прикладных технологий и систем	
Владеть:	

ОПК-2-В1 методами проектирования прикладных технологий и систем

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы
	Раздел 1. Основы информационной безопасности и защиты информации							
1.1	Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Обзор и сравнительный анализ стандартов информационной безопасности. Исследование причин нарушений безопасности. Понятие политики безопасности. Реализация и гарантирование политики безопасности. Принципы организации системы защиты, направления, способы и методы защиты. /Лек/	7	8	ОПК-2-В1	Л1.3 Л1.4Л2.1 Л2.3 Л2.4Л3.1 Э1 Э2 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в электронном курсе: Основные понятия и определения. Современное состояние и перспективы развития защиты информации. Общая проблема информационной безопасности информационных систем. /Ср/	7	16	ПК-1-31	Л1.3 Л1.4Л2.1 Л2.3 Л2.4Л3.1 Э1 Э2 Э3 Э4			
1.3	Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Состав и назначение должностных инструкций. /Пр/	7	5	ОПК-2-У1 ОПК-2-В1	Л1.1Л2.1Л3.1 Э2 Э4		КМ1	Р1

1.4	Исследование и изучение структуры средств безопасности операционных систем и использование их для конфиденциального доступа к информации. Разработка и реализация алгоритма функционирования системы безопасности объектов. /Лаб/	7	4	ОПК-2-У1 ОПК-2-В1	Л1.3 Л1.4Л2.1 Л2.3 Л2.4Л3.1 Э1 Э2 Э3 Э4			Р3
Раздел 2. Модели безопасности в компьютерных системах								
2.1	Модели безопасного субъектного взаимодействия в компьютерной системе. Процедура идентификации и аутентификации. Сопряжение защитных механизмов. Архитектура защищенных операционных систем. Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе. /Лек/	7	8	ОПК-2-В1	Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
2.2	Самостоятельное изучение учебного материала в электронном курсе: Аутентификация пользователей. Формализация задачи сопряжения. Методы сопряжения. Типизация данных, необходимых для обеспечения работы средств сопряжения. Понятие внешнего разделяемого сервиса безопасности. Постановка задачи. Понятие и свойства модуля реализации защитных функций. /Ср/	7	10	ОПК-2-У1	Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
2.3	Разработка и реализация алгоритма функционирования системы безопасности субъектов. Проектирование модуля реализации защитных функций в среде гарантирования политики безопасности. Методика проверки попарной корректности субъектов при проектировании механизмов обеспечения безопасности с учетом передачи параметров. /Лаб/	7	5	ОПК-2-В1	Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			Р4
Раздел 3. Защита информации в компьютерных сетях								

3.1	Особенности обеспечения информационной безопасности в компьютерных сетях. Специфика средств защиты в компьютерных сетях. Сетевые модели передачи данных. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP. Модель взаимодействия открытых систем OSI/ISO. Современные средства построения защищенных виртуальных сетей. /Лек/	7	10	ОПК-2-У1	Л1.3 Л1.4Л2.1 Л2.2 Л2.4Л3.1 Э1 Э2 Э3 Э4			
3.2	Самостоятельное изучение учебного материала в электронном курсе: Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO. Адресация в глобальных сетях. Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. /Ср/	7	10	ОПК-2-У1	Л1.3 Л1.4Л2.1 Л2.2 Л2.4Л3.1 Э1 Э2 Э3 Э4			
3.3	Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. /Пр/	7	6	ОПК-2-В1 ПК-1-31	Л1.1Л2.1Л3.1 Э1			
3.4	Разработка и реализация алгоритма сетевого фильтра. Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. /Лаб/	7	4	ОПК-2-У1	Л1.3 Л1.4Л2.1 Л2.2 Л2.4Л3.1 Э1 Э2 Э3 Э4			P5
	Раздел 4. Методы и системы защиты информации							

4.1	Защита информации от несанкционированного доступа. Каналы утечки информации. Системы анализа защищённости и обнаружения вторжений. Модели и источники каналов утечки информации. Способы несанкционированного доступа к информации. Компьютерные средства реализации защиты в информационных системах. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись. /Лек/	7	8	ОПК-2-У1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
4.2	Самостоятельное изучение учебного материала в электронном курсе: Причины нарушения целостности информации. Функции непосредственной защиты информации. Задачи защиты информации. Методы и системы защиты информации. Аппаратные средства защиты. Программные средства защиты. Криптографические средства защиты. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/	7	36	ОПК-2-У1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			Р6
4.3	Программные средства защиты. Криптографические средства защиты. /Пр/	7	6	ОПК-2-У1	Л1.1Л2.1Л3. 1 Э2 Э4			Р2
4.4	Разработка и реализация алгоритма криптографического преобразования. Источники и защита от несанкционированного доступа. /Лаб/	7	4	ОПК-2-У1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			Р5
4.5	Проведение зачета с оценкой /ЗачётСоц/	7	4		Э1 Э2 Э3 Э4			