Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Котова Лариса Анатольевна
Должность: Директор филиала
Дата подписания: 17.05.2024 10:42:56
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

Информационная безопасность

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:
аудиторные занятия 54
самостоятельная работа 63
часов на контроль 27

Формы контроля в семестрах:
экзамен 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	10			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Практические	18	18	18	18
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	63	63	63	63
Часы на контроль	27	27	27	27
Итого	144	144	144	144

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Цели освоения дисциплины: формирование у обучающихся системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.
1.2	Задачи:
1.3	- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;
1.4	- изучить основы защиты информации, а также методы, средства и инструменты шифрования, применяемых в сфере информационных технологий и бизнеса;
1.5	- получить навыки работы с методами шифрования и криптоанализа.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Блок ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Интеллектуальные технологии в металлургии
2.1.2	Интеллектуальные технологии в энергетике
2.1.3	Научно-исследовательская работа
2.1.4	Управление техническими системами
2.1.5	Моделирование металлургических процессов с использованием современных программных продуктов
2.1.6	Электротехника, электроника и схемотехника
2.1.7	Операционные системы
2.1.8	Учебная практика по получению первичных профессиональных умений
2.1.9	Архитектура ЭВМ и систем
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

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-З1 принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
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
Знать:
ОПК-3-З1 принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
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
Уметь:
ОПК-3-У1 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
Владеть:
ОПК-3-В1 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публи-каций, и библиографии по научноисследовательской работе с учетом требований информацион-ной безопасности

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. Введение, основы информационной безопасности							
1.1	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Основные нормативно-правовые акты в области информационной безопасности. /Лек/	8	5	ОПК-3-У1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э2 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в электронном курсе: Информация. Её виды и свойства. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. /Лаб/	8	11	ОПК-3-З1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э2 Э3 Э4			
1.3	Методы и средства организационно-правовой защиты информации. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. /Пр/	8	7	ОПК-3-В1	Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	Раздел 2. Экономическая безопасность предприятия							
2.1	Экономическая безопасность предприятия. Инженерная защита объектов. Защита информации от утечки по техническим каналам. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. /Лек/	8	5	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э3 Э4			

2.2	Самостоятельное изучение учебного материала в электронном курсе: Коммерческая тайна. Персональные данные. Служебная тайна. Профессиональная тайна. Угрозы информационной безопасности. Классификация угроз. Каналы утечки информации. Модель нарушителя информационной безопасности. Классификация средств защиты информации. /Ср/	8	22		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э3 Э4			
2.3	Анализ возможных каналов утечки информации. Защита документооборота в вычислительных системах. /Пр/	8	7	ПК-1-З1 ОПК-3-У1	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	Раздел 3. Криптографические методы защиты информации							
3.1	Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы. /Лек/	8	4		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
3.2	Самостоятельное изучение учебного материала в электронном курсе: Основные этапы развития криптологии. Основные понятия и определения. Криптостойкость. Методы криптографического преобразования данных. Кодирование. Асимметричные системы шифрования RSA. Надежность использования криптосистем. Перспективы развития криптографических методов защиты информации. /Ср/	8	16		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			

3.3	Шифрование текста по ключу методами замены, перестановки, аддитивными методами (гаммированием). Методы шифрования текста при помощи аналитических преобразований. /Пр/	8	4		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			
	Раздел 4. Методы и средства защиты информации							
4.1	Методы парольной защиты. Использование простого пароля. Использование динамически изменяющегося пароля. Методы идентификации и аутентификации пользователей. Идентификация, аутентификация с помощью биометрических данных. Использование средств стеганографии для защиты файлов. Создание защищенного канала связи средствами виртуальной частной сети. Антивирусные средства защиты информации. /Лек/	8	4		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
4.2	Самостоятельное изучение учебного материала в электронном курсе: Классификация существующих типов систем обнаружения атак (СОА). Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ. Пароли как средство защиты информации. Системы и средства генерации паролей и их недостатки. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/	8	25		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
4.3	Разработка программной парольной защиты. Количественная оценка стойкости парольной защиты. Диагностика антивирусной программы и создание тестовых вирусов. /Лаб/	8	3		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			
4.4	Экзамен /Лаб/	8	4		Э1 Э2 Э3 Э4			