

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Котова Лариса Анатольевна
Должность: Директор филиала
Дата подписания: 17.08.2024 10:16:17
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 **заочная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144	Формы контроля на курсах: экзамен 5
в том числе:		
аудиторные занятия	24	
самостоятельная работа	111	
часов на контроль	9	

Распределение часов дисциплины по курсам

Курс	5		Итого	
	уп	рп		
Лекции	8	8	8	8
Лабораторные	10	10	10	10
Практические	6	6	6	6
Итого ауд.	24	24	24	24
Контактная работа	24	24	24	24
Сам. работа	111	111	111	111
Часы на контроль	9	9	9	9
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	
1.3	Задачи:
1.4	- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;
1.5	- изучить основы защиты информации, а также методы, средства и инструменты шифрования, применяемых в сфере информационных технологий и бизнеса;
1.6	- 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	Моделирование металлургических процессов с использованием современных программных продуктов	
2.1.4	Управление техническими системами	
2.1.5	Электротехника, электроника и схемотехника	
2.1.6	Вычислительные системы, сети и телекоммуникации	
2.1.7	Компьютерная графика	
2.1.8	Языки программирования	
2.1.9	Архитектура ЭВМ и систем	
2.1.10	Информатика	
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-1-31 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-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 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-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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	
Владеть:	
ОПК-2-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. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. /Лек/	5	4	ПК-1-31 ПК-1-У1 ОПК-2-У1 ОПК-2-В1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в электронном курсе: Информация. Её виды и свойства. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность. /Ср/	5	20	ОПК-2-В1	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э3 Э4			
1.3	Методы и средства организационно-правовой защиты информации. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. /Лаб/	5	2		Л1.1 Л1.2 Л1.3Л2.2 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			Р1
	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/	5	1		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/	5	26	ОПК-2-31	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.6 Э1 Э2 Э4			
2.3	Составление плана и основных положений политики безопасности для учреждения. /Лаб/	5	2		Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.6Л3.1 Э1 Э2 Э3 Э4			P2
2.4	Анализ возможных каналов утечки информации. Защита документооборота в вычислительных системах. /Пр/	5	2	ОПК-2-В1	Л1.2Л2.3 Э2 Э4			P5
	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. Криптоанализ и атаки на криптосистемы. /Лек/	5	1	ПК-1-31 ОПК-2-У1	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. /Ср/	5	22		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			

3.3	Асимметричные системы шифрования RSA. Надежность использования криптосистем. Перспективы развития криптографических методов защиты информации. /Пр/	5	2					P6
3.4	Шифрование текста по ключу методами замены. Шифрование текста по ключу методами перестановки. Методы шифрования текста при помощи аналитических преобразований. Шифрование текста по ключу аддитивными методами (гаммированием). Шифры с открытым ключом. Алгоритм RSA. /Лаб/	5	2		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			P3
	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/	5	2		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. Методы защиты от вредоносных программ. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/	5	34		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э2 Э3 Э4			
4.3	Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. /Пр/	5	1		Л1.1Л2.1 Э2 Э4			P7

4.4	Основы работы антивирусных программ. Пароли как средство защиты информации. Системы и средства генерации паролей и их недостатки. /Пр/	5	1		Л1.1Л2.2 Э2 Э4			Р8
4.5	Методы парольной защиты. Разработка программной парольной защиты. Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требуемой стойкостью к взлому. Генератор паролей, обладающий требованиями к парольным генераторам. Диагностика антивирусной программы и создание тестовых вирусов. /Лаб/	5	4		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			Р4
4.6	Проведение экзамена /Ср/	5	9		Э1 Э2 Э3 Э4		КМ1	