

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Котова Лариса Анатольевна
Должность: Директор филиала
Дата подписания: 14.09.2023 15:55:03
Уникальный программный ключ:
10730ffe6b1ed036b744b6a9d97700b86e5c04a7

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

Защита информации

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 **5 ЗЕТ**

Часов по учебному плану	180	Формы контроля на курсах: зачет с оценкой 4
в том числе:		
аудиторные занятия	18	
самостоятельная работа	158	
часов на контроль	4	

Распределение часов дисциплины по курсам

Курс	4		Итого	
	уп	рп		
Лекции	6	34	6	34
Практические	12	17	12	17
Итого ауд.	18	68	18	68
Контактная работа	18	68	18	68
Сам. работа	158	108	158	108
Часы на контроль	4	4	4	4
Итого	180	180	180	180

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	CASE-технологии	
2.1.2	Программная инженерия	
2.1.3	Информационные системы и технологии	
2.1.4	Учебная практика по получению первичных профессиональных умений	
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Подготовка к процедуре защиты и защита выпускной квалификационной работы	
2.2.2	Преддипломная практика	
2.2.3	Разработка интернет-приложений на клиентской стороне	
2.2.4	Управление IT-структурами предприятий	
2.2.5	Управление проектами	
2.2.6	Языки и среды разработки интернет-приложений	

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ

ПК-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС	
Знать:	
ПК-2-31 информационное обеспечение и принципы построения информационных систем управления технологическими процессами	
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-3-31 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-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС	
Уметь:	
ПК-2-У1 использовать методы системного моделирования технологических процессов	
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	
ПК-2: Способен выполнять проектные работы по созданию, модификации (интегрированию программных модулей) и сопровождению ИС, формулировать требования к ИС	
Владеть:	

ПК-2-В1 современными компьютерными методами математического моделирования технологических процессов

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

Владеть:

ОПК-3-В1 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научноисследовательской работе с учетом требований информационной 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. 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/	4	8		Л1.3 Л1.4Л2.1 Л2.3 Л2.4 Э1 Э2 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в LMS Canvas: Основные понятия и определения. Современное состояние и перспективы развития защиты информации. Общая проблема информационной безопасности информационных систем. /Ср/	4	26		Л1.3 Л1.4Л2.1 Л2.3 Л2.4 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/	4	5		Л1.1Л2.1 Э2 Э4			

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/	4	4		Л1.3 Л1.4Л2.1 Л2.3 Л2.4Л3.1 Э1 Э2 Э3 Э4			
Раздел 2. Модели безопасности в компьютерных системах								
2.1	Модели безопасного 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/	4	8		Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
2.2	Самостоятельное изучение учебного материала в LMS Canvas: 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/	4	20		Л1.3 Л1.4Л2.1 Л2.4 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/	4	5		Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
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/	4	10		Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Э1 Э2 Э3 Э4			
3.2	Самостоятельное изучение учебного материала в LMS Canvas: 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/	4	20		Л1.3 Л1.4Л2.1 Л2.2 Л2.4 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/	4	6		Л1.1Л2.1			
3.4	Разработка и реализация алгоритма сетевого фильтра. Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. /Лаб/	4	4		Л1.3 Л1.4Л2.1 Л2.2 Л2.4Л3.1 Э1 Э2 Э3 Э4			
	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/	4	8		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
4.2	Самостоятельное изучение учебного материала в LMS Canvas: 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/	4	42		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
4.3	Программные средства защиты. Криптографические средства защиты. /Пр/	4	6		Л1.1Л2.1 Э2 Э4			
4.4	Разработка и реализация алгоритма криптографического преобразования. Источники и защита от несанкционированного доступа. /Лаб/	4	4		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
4.5	Проведение зачета с оценкой /ЗачётСОц/	4	4		Э1 Э2 Э3 Э4			