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

Квалификация **Бакалавр**
Форма обучения **очная**
Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 68
самостоятельная работа 76

Формы контроля в семестрах:
зачет с оценкой 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	34	34	34	34
Лабораторные	34	34	34	34
В том числе инт.	34	34	34	34
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.05
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	CASE-технологии
2.1.2	Программная инженерия
2.1.3	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
2.1.4	Решение прикладных задач с использованием MATLAB
2.1.5	Электротехника, электроника и схемотехника
2.1.6	Алгоритмы теории игр
2.1.7	Базы данных
2.1.8	Металлургические технологии
2.1.9	Общая энергетика
2.1.10	Проектный подход в технике
2.1.11	Технологии программирования
2.1.12	Численные методы
2.1.13	Вычислительные системы, сети и телекоммуникации
2.1.14	Теория вероятностей и математическая статистика
2.1.15	Языки программирования
2.1.16	Информационные системы и технологии
2.1.17	Начертательная геометрия и инженерная графика
2.1.18	Информатика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Интеллектуальные технологии в металлургии
2.2.2	Интеллектуальные технологии в энергетике
2.2.3	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.4	Преддипломная практика
2.2.5	Средства информатизации в металлургии
2.2.6	Средства информатизации в энергетике

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
УК-6: Принятие решений (способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; управлять своей профессиональной деятельностью или проектами в соответствующей профессиональной сфере, брать на себя ответственность за принятие решений)
Знать:
УК-6-З2 основные методы и модели обеспечения и управления информационной безопасностью, методы управления рисками информационной безопасности
УК-6-З1 задачи информационной безопасности, основные тенденции и направления формирования и функционирования комплексной системы защиты информации
УК-3: Проектирование и разработка (способен: проектировать и разрабатывать продукцию, процессы и системы, соответствующие профилю образовательной программы; выбирать и применять соответствующие методики проектирования и разработки, включая передовые методы и технологии)

Знать:
УК-3-З1 принципы построения современных систем защиты информации в компьютерных сетях
ПК-2: Способен проектировать прикладные технологии и системы
Знать:
ПК-2-З1 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-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
УК-6: Принятие решений (способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; управлять своей профессиональной деятельностью или проектами в соответствующей профессиональной сфере, брать на себя ответственность за принятие решений)
Уметь:
УК-6-У1 проводить анализ возможности применения моделей систем защиты информации различного назначения
УК-6-У2 Уровень 2 проводить сравнительный анализ параметров систем защиты информации, определять оптимальные типы криптографических протоколов при передаче информации.
УК-3: Проектирование и разработка (способен: проектировать и разрабатывать продукцию, процессы и системы, соответствующие профилю образовательной программы; выбирать и применять соответствующие методики проектирования и разработки, включая передовые методы и технологии)
Уметь:
УК-3-У1 определять применяемые методы несанкционированного доступа к данным
ПК-2: Способен проектировать прикладные технологии и системы
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
УК-6: Принятие решений (способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; управлять своей профессиональной деятельностью или проектами в соответствующей профессиональной сфере, брать на себя ответственность за принятие решений)
Владеть:
УК-6-В2 методами и средствами технической защиты информации, методами расчета и инструментального контроля показателей технической защиты информации
УК-6-В1 навыками обоснования решений по выбору и применению моделей систем защиты информации различного назначения
УК-3: Проектирование и разработка (способен: проектировать и разрабатывать продукцию, процессы и системы, соответствующие профилю образовательной программы; выбирать и применять соответствующие методики проектирования и разработки, включая передовые методы и технологии)
Владеть:
УК-3-В1 навыками отслеживания несанкционированного доступа к данным и установки защиты данных
ПК-2: Способен проектировать прикладные технологии и системы
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, 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. 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		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. 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. /Ср/	7	12		Л1.3 Л1.4Л2.1 Л2.3 Л2.4 Э1 Э2 Э3 Э4			

1.3	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	8		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 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		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/	7	8		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/	7	10		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/	7	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/	7	10		Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Э1 Э2 Э3 Э4			
3.3	Разработка и реализация алгоритма сетевого фильтра. Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. /Лаб/	7	8		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/	7	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/	7	42		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
4.3	Разработка и реализация алгоритма криптографического преобразования. Источники и защита от несанкционированного доступа. /Лаб/	7	8		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
4.4	Проведение зачета с оценкой /ЗачётСОц/	7	4		Э1 Э2 Э3 Э4			