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

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: 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.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-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 основные понятия информационной безопасности, виды и источники угроз безопасности информации
УК-3-З2 нормативно-правовые документы в области информационной безопасности, основные требования 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)

Знать:
УК-6-З1 основные методы и средства управления информационной безопасностью в профессиональной деятельности
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-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 актуальные источники угроз безопасности для различных профессиональных областей
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 выбирать методы и средства защиты информации, анализировать информационную безопасность многопользовательских систем
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 проектировать прикладные технологии и системы
Уметь:
ПК-2-У1 использовать методы системного моделирования технологических процессов
Владеть:
ПК-2-В1 современными компьютерными методами математического моделирования технологических процессов
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-В1 навыками проведения анализа степени защищенности информации и осуществления повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем
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
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 разработки моделей злоумышленника и угроз информационной безопасности предприятия

УК-3-В2 разработки политики безопасности, используя известные подходы, методы и средства

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/	7	8		Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.4 Л2.6 Э1 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в LMS Canvas: Информация. Её виды и свойства. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность. /Ср/	7	8		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/	7	8		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/	7	8		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 LMS Canvas: 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/	7	12		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. Анализ возможных каналов утечки информации. Защита документооборота в вычислительных системах. /Лаб/	7	8		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/	7	10		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
3.2	Самостоятельное изучение учебного материала в LMS Canvas: 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/	7	12		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			

3.3	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/	7	10		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/	7	8		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э1 Э2 Э3 Э4			
4.2	Самостоятельное изучение учебного материала в LMS Canvas: 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/	7	40		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6 Э2 Э3 Э4			

4.3	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/	7	8		Л1.1 Л1.2 Л1.3Л2.4 Л2.5 Л2.6Л3.1 Э1 Э2 Э3 Э4			
4.4	Проведение зачета с оценкой /ЗачётСОц/	7	4		Э1 Э2 Э3 Э4			