МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский технологический университет «МИСИС»

Аннотация рабочей программы учебной дисциплины

Информационная безопасность

Закреплена за подразделением Кафедра инфокоммуникационных технологий

Направление подготовки 09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Профиль

Квалификация **Бакалавр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 51
самостоятельная работа 22
часов на контроль 35

Формы контроля в семестрах:
экзамен 4

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	17	17	17	17
Лабораторные	17	17	17	17
Практические	17	17	17	17
Итого ауд.	51	51	51	51
Контактная работа	51	51	51	51
Сам. работа	22	22	22	22
Часы на контроль	35	35	35	35
Итого	108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Целями освоения дисциплины являются формирование у студентов знаний по основам инженерно-технической защиты информации, обеспечения конфиденциальности, целостности и доступности данных, а также навыков и умений в области анализа потенциальных угроз информационной безопасности, выборе средств реализации защиты в информационных системах.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
	Блок ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**	
2.1.1	Базы данных	
2.1.2	Объектно-ориентированное программирование	
2.1.3	Персональная эффективность	
2.1.4	Введение в специальность	
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	Подготовка к процедуре защиты и защита выпускной квалификационной работы	

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
УК-3: Способен эффективно обмениваться информацией, идеями, проблемами и решениями с инженерным сообществом и обществом в целом, осуществлять социальное взаимодействие и реализовывать свою роль в команде
Знать:
УК-3-З1 Основные типы вредоносных программ; методы защиты от компьютерных вирусов и других вредоносных программ; принципы сетевого экранирования; технологии построения обманных систем; основные технические каналы утечек информации; виды оборудования для защиты от утечек по техническим каналам.
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 Основные понятия и определения в области информационной безопасности; источники, риски и формы атак на информационные системы; угрозы, которым подвергается информация; основные направления защиты информации; основные законодательные акты РФ в области информационной безопасности; ответственность за преступления в сфере компьютерной безопасности.
УК-2: Способен собирать и интерпретировать данные и определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, умение обосновывать принятые решения
Знать:
УК-2-З1 Основные определения и принципы криптографии; наиболее распространенные симметричные и асимметричные криптографические алгоритмы; требования к криптографическим хэш-функциям; алгоритмы электронной цифровой подписи и атаки на них; сущность и алгоритм реализации протокола с нулевым разглашением; основные положения стеганографии; применение цифровых водяных знаков для защиты интеллектуальной собственности.
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 Выявлять источники, риски и формы атак на информацию; применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации информационной безопасности.
УК-3: Способен эффективно обмениваться информацией, идеями, проблемами и решениями с инженерным сообществом и обществом в целом, осуществлять социальное взаимодействие и реализовывать свою роль в команде
Уметь:
УК-3-У1 Сопоставлять различные виды вредоносного программного обеспечения и выбирать адекватные меры программно-аппаратной реализации средств защиты; определять возможные причины и пути утечек информации через сетевые экраны; рассчитывать расстояние до границы контролируемой зоны, требуемое для передачи конфиденциальной

информации по электромагнитному каналу; выбирать средства защиты информации, необходимые для предотвращения её утечек по техническим каналам.
УК-2: Способен собирать и интерпретировать данные и определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, умение обосновывать принятые решения
Уметь:
УК-2-У1 Выбирать алгоритм криптографической защиты в соответствии с характером защищаемой информации; выполнять первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены; производить генерацию открытого и закрытого ключа и шифрование в алгоритмах RSA и ELGAMAL; находить хэш-образ заданного сообщения; проверять подлинность электронной цифровой подписи по схеме RSA.
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 определения критериев оценки безопасности сообщения, передаваемого по электромагнитному каналу; методикой организации защиты проводных линий от утечки информации; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.
УК-2: Способен собирать и интерпретировать данные и определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, умение обосновывать принятые решения
Владеть:
УК-2-В1 Владеть навыками шифрования информации, генерации открытых и закрытых ключей, вычисления значений хэш-функций и электронной цифровой подписи; навыками применения стеганографических методов и программ в задачах защиты информации.