МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Аннотация рабочей программы учебной дисциплины

Современные технологии защиты информации

Закреплена за подразделением — Кафедра инфокоммуникационных технологий

Направление подготовки — 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Профиль — Промдизайн и инжиниринг

Квалификация **Магистр**
Форма обучения **очная**
Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 34
самостоятельная работа 104
часов на контроль 42

Формы контроля в семестрах:
экзамен 1
курсовая работа 1

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	9	9	9	9
Практические	25	25	25	25
Итого ауд.	34	34	34	34
Контактная работа	34	34	34	34
Сам. работа	104	104	104	104
Часы на контроль	42	42	42	42
Итого	180	180	180	180

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Целью освоения дисциплины является обучение студентов методам обеспечения защиты информации в современных информационных системах (ИС), функционирующих в условиях внешних и внутренних угроз информационной безопасности. Это даст возможность будущему магистру глубоко понимать функционирование механизмов защиты информации в современных ИС, а также решать вопросы формирования политики безопасности, возникающие в ходе проектирования и эксплуатации перспективных ИС. Студенты будут уметь выбирать необходимые протоколы безопасности и предлагать современные методы защиты от новых угроз информационной безопасности; применять методы защиты цифрового контента от угроз модификации и несанкционированного использования при построении ИС; разрабатывать методики построения программной и аппаратной реализации защиты корпоративной сети с учетом применения облачных технологий; моделировать работу алгоритмов защиты информации на базе математического аппарата динамических дискретных систем; анализировать риски функционирования систем защиты информации.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Блок ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Архитектурно-строительная визуализация с применением CAD-систем
2.2.2	Дизайн процесс
2.2.3	Методологии дизайна
2.2.4	Научно-исследовательская работа
2.2.5	Основы интеграции и карбоноэффективное проектирование технологических процессов
2.2.6	Производственная практика
2.2.7	Твердотельное моделирование цифровых сборок
2.2.8	Технологии и материалы
2.2.9	Управление человеческими ресурсами в проектной деятельности
2.2.10	CAD моделирование в дизайне
2.2.11	Колористика в дизайне
2.2.12	Компьютерное моделирование и инжиниринг промышленных объектов
2.2.13	Педагогическая практика
2.2.14	Поверхностное моделирование: построение моделей класса B и C
2.2.15	Программирование в Unreal и Unity
2.2.16	Проектирование IOT
2.2.17	Эскизное моделирование
2.2.18	Авторское право в промышленном дизайне
2.2.19	Деловая презентационная графика
2.2.20	Лидерство и управление командой проекта
2.2.21	Поверхностное моделирование класса A
2.2.22	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.23	Преддипломная практика

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
ОПК-4: Способен применять на практике новые научные принципы и методы исследований
Знать:
ОПК-4-З2 Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации
ОПК-4-З1 Современные методы криптографической и стеганографической защиты информации
ОПК-3: Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями
Знать:
ОПК-3-З1 Методы защиты программного обеспечения от угроз информационной безопасности, методы защиты авторских прав на цифровой контент

УК-2: Способен интегрировать знания и принимать решения в сложных ситуациях, формулировать суждения на основе неполной или ограниченной информации, управлять проектом на всех этапах его жизненного цикла
Знать:
УК-2-З2 Основные методики анализа рисков информационной безопасности на предприятии
УК-1: Способен осуществлять критический анализ новых и сложных инженерных объектов, процессов и систем в междисциплинарном контексте, проблемных ситуаций на основе системного подхода, выбрать и применить наиболее подходящие и актуальные методы из существующих аналитических, вычислительных и экспериментальных методов или новых и инновационных методов, вырабатывать стратегию действий
Знать:
УК-1-З1 Методы моделирования поведения нарушителя информационной безопасности. Принципы построения и функционирования сетей Петри
УК-2: Способен интегрировать знания и принимать решения в сложных ситуациях, формулировать суждения на основе неполной или ограниченной информации, управлять проектом на всех этапах его жизненного цикла
Знать:
УК-2-З1 Алгоритмы принятия решений при проектировании системы защиты информации на основе закона Парето и метода достижимых целей.
ОПК-4: Способен применять на практике новые научные принципы и методы исследований
Уметь:
ОПК-4-У1 Применять простейшие методы шифрования и дешифрования текстовой информации, использовать протоколы разделения и разбиения секрета
ОПК-3: Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями
Уметь:
ОПК-3-У1 Производить встраивание цифровых водяных знаков в мультимедийные и программные файлы
УК-2: Способен интегрировать знания и принимать решения в сложных ситуациях, формулировать суждения на основе неполной или ограниченной информации, управлять проектом на всех этапах его жизненного цикла
Уметь:
УК-2-У1 Применять методы Парето-оптимизации в системе поддержки принятия решений в области проектирования системы защиты информации на предприятии
УК-1: Способен осуществлять критический анализ новых и сложных инженерных объектов, процессов и систем в междисциплинарном контексте, проблемных ситуаций на основе системного подхода, выбрать и применить наиболее подходящие и актуальные методы из существующих аналитических, вычислительных и экспериментальных методов или новых и инновационных методов, вырабатывать стратегию действий
Уметь:
УК-1-У1 Моделировать поведение нарушителя с помощью сети Петри
ОПК-4: Способен применять на практике новые научные принципы и методы исследований
Уметь:
ОПК-4-У2 Производить расчет критической длины линии связи при PNS-атаке на квантовый канал
УК-2: Способен интегрировать знания и принимать решения в сложных ситуациях, формулировать суждения на основе неполной или ограниченной информации, управлять проектом на всех этапах его жизненного цикла
Уметь:
УК-2-У2 Использовать концепцию управления рисками при анализе защищенности инфокоммуникационной структуры предприятия
ОПК-4: Способен применять на практике новые научные принципы и методы исследований
Владеть:
ОПК-4-В1 Методикой генерации псевдослучайных последовательностей для дальнейшего использования в криптографических алгоритмах
УК-2: Способен интегрировать знания и принимать решения в сложных ситуациях, формулировать суждения на основе неполной или ограниченной информации, управлять проектом на всех этапах его жизненного цикла
Владеть:
УК-2-В1 Методикой анализа рисков информационной безопасности при построении системы защиты информации