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 — 09.04.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Профиль — Цифровые двойники в технических системах

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

Часов по учебному плану 180
в том числе:
аудиторные занятия 34
самостоятельная работа 92
часов на контроль 54

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	92	92	92	92
Часы на контроль	54	54	54	54
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	Алгоритмизация и программирование
2.2.2	Интеллектуальный анализ данных
2.2.3	Методы разработки высокопроизводительных программ
2.2.4	Научно-исследовательская работа
2.2.5	Производственная практика
2.2.6	Цифровое представление физических производственных элементов
2.2.7	Цифровые технологии трансформации бизнеса
2.2.8	Алгоритмы искусственного интеллекта в управлении и прогнозировании
2.2.9	Инструменты разработки цифровых двойников
2.2.10	Научно-исследовательская работа. Проектирование информационных систем
2.2.11	Создание графических интерфейсов цифровых двойников
2.2.12	Технология разработки цифровых двойников технологических процессов
2.2.13	Диагностика и мониторинг технических систем
2.2.14	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.15	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-З1 Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации
ОПК-2: Способен проектировать и разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач в условиях неопределенности и альтернативных решений в рамках междисциплинарных областей
Знать:
ОПК-2-З1 Современные методы криптографической и стеганографической защиты информации
УК-3: Способен использовать различные методы ясного и недвусмысленного формулирования своих выводов, знаний и обоснований для специализированной и неспециализированной аудиторий в национальном и международном контекстах, организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Знать:
УК-3-З1 Типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы обеспечения информационной безопасности управления предприятием; принципы защиты информации и обеспечения информационной безопасности, сведения об основных угрозах информационной безопасности и их источниках

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
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-2: Способен проектировать и разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач в условиях неопределенности и альтернативных решений в рамках междисциплинарных областей
Уметь:
ОПК-2-У1 Производить встраивание цифровых водяных знаков в мультимедийные и программные файлы
УК-3: Способен использовать различные методы ясного и недвусмысленного формулирования своих выводов, знаний и обоснований для специализированной и неспециализированной аудиторий в национальном и международном контекстах, организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уметь:
УК-3-У1 Использовать концепцию управления рисками при анализе защищенности инфокоммуникационной структуры предприятия
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-3: Способен использовать различные методы ясного и недвусмысленного формулирования своих выводов, знаний и обоснований для специализированной и неспециализированной аудиторий в национальном и международном контекстах, организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Уметь:
УК-3-У2 Анализировать угрозы информационной безопасности и уязвимости систем защиты информации, строить модель информационной безопасности с полным перекрытием угроз
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-3: Способен использовать различные методы ясного и недвусмысленного формулирования своих выводов, знаний и обоснований для специализированной и неспециализированной аудиторий в национальном и международном контекстах, организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
Владеть:
УК-3-В1 Методикой анализа рисков информационной безопасности при построении системы защиты информации