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 — Прикладная информатика в цифровой экономике

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

Часов по учебному плану 108
в том числе:
аудиторные занятия 34
самостоятельная работа 74

Формы контроля в семестрах:
зачет 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	74	74	74	74
Итого	108	108	108	108

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	Методология моделирования и совершенствования бизнес-процессов предприятия
2.2.2	Проектно-продуктовая трансформация в корпоративных информационных системах
2.2.3	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
2.2.4	Управление инновационными и инвестиционными проектами в сфере ИКТ
2.2.5	Экономика информационных систем
2.2.6	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.7	Роботизация бизнес-процессов (RPA)

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Знать:
ПК-3-З1 Основные методики анализа рисков информационной безопасности на предприятии
ПК-3-З3 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
ПК-3-З2 Методы моделирования поведения нарушителя информационной безопасности. Принципы построения и функционирования сетей Петри
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Знать:
ОПК-5-З2 Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации
ОПК-5-З1 Современные методы криптографической и стеганографической защиты информации
ОПК-5-З3 Методы защиты программного обеспечения от угроз информационной безопасности, методы защиты авторских прав на цифровой контент
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Уметь:
ПК-3-У2 Анализировать угрозы информационной безопасности и уязвимости систем защиты информации, строить модель информационной безопасности с полным перекрытием угроз
ПК-3-У1 Использовать концепцию управления рисками при анализе защищенности инфокоммуникационной структуры предприятия
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Уметь:

ОПК-5-У2 Производить расчет критической длины линии связи при PNS-атаке на квантовый канал
ОПК-5-У1 Применять простейшие методы шифрования и дешифрования текстовой информации, использовать протоколы разделения и разбиения секрета
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Уметь:
ПК-3-У3 Применять методы Парето-оптимизации в системе поддержки принятия решений в области проектирования системы защиты информации на предприятии
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Уметь:
ОПК-5-У3 Производить встраивание цифровых водяных знаков в мультимедийные и программные файлы
ПК-3: Способен проводить анализ и реинжиниринг бизнес-процессов, осуществлять проектирование и поддержку архитектуры и прототив ИС
Владеть:
ПК-3-В1 Методикой анализа рисков информационной безопасности при построении системы защиты информации
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
Владеть:
ОПК-5-В1 Методикой генерации псевдослучайных последовательностей для дальнейшего использования в криптографических алгоритмах