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 — Искусственный интеллект и машинное обучение

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

Часов по учебному плану 180
в том числе:
аудиторные занятия 34
самостоятельная работа 110
часов на контроль 36

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	110	110	110	110
Часы на контроль	36	36	36	36
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	Инженерия машинного обучения
2.2.2	Искусственный интеллект в задачах распознавания образов
2.2.3	Методология DevOps в машинном обучениии
2.2.4	Научно-исследовательская практика
2.2.5	Производственная практика
2.2.6	Интеллектуальные мультиагентные системы
2.2.7	Искусственный интеллект в компьютерных играх
2.2.8	Искусственный интеллект в медицине
2.2.9	Искусственный интеллект в финансовых технологиях
2.2.10	Научно-исследовательская работа
2.2.11	Правовые аспекты использования искусственного интеллекта
2.2.12	Современные устройства центров обработки больших данных и нейросетевых процессоров
2.2.13	Экспертные и рекомендательные, информационно-аналитические системы
2.2.14	Методы искусственного интеллекта в робототехнических системах
2.2.15	Подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.16	Преддипломная практика
2.2.17	Блокчейн-технологии
2.2.18	Искусственный интеллект в задачах обработки естественного языка
2.2.19	Современные интеллектуальные сетевые сервисы

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
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-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
ОПК-7: Способен использовать методы научных исследований и математического моделирования в области проектирования и управления информационными системами, осуществлять моделирование, анализ и эксперименты в целях проведения детального исследования для решения сложных задач в профессиональной области
Знать:
ОПК-7-З2 Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации
ОПК-7-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-З2 Методы моделирования поведения нарушителя информационной безопасности. Принципы построения и функционирования сетей Петри
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 Методы защиты программного обеспечения от угроз информационной безопасности, методы защиты авторских прав на цифровой контент
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 Основные методики анализа рисков информационной безопасности на предприятии
ОПК-7: Способен использовать методы научных исследований и математического моделирования в области проектирования и управления информационными системами, осуществлять моделирование, анализ и эксперименты в целях проведения детального исследования для решения сложных задач в профессиональной области
Уметь:
ОПК-7-У1 Применять простейшие методы шифрования и дешифрования текстовой информации, использовать протоколы разделения и разбиения секрета
ОПК-7-У2 Производить расчет критической длины линии связи при PNS-атаке на квантовый канал
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-У4 Моделировать поведение нарушителя с помощью сети Петри
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
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 Использовать концепцию управления рисками при анализе защищенности инфокоммуникационной структуры предприятия
ОПК-3-У2 Анализировать угрозы информационной безопасности и уязвимости систем защиты информации, строить модель информационной безопасности с полным перекрытием угроз
ОПК-3-У3 Применять методы Парето-оптимизации в системе поддержки принятия решений в области проектирования системы защиты информации на предприятии
ОПК-7: Способен использовать методы научных исследований и математического моделирования в области проектирования и управления информационными системами, осуществлять моделирование, анализ и эксперименты в целях проведения детального исследования для решения сложных задач в профессиональной области
Владеть:
ОПК-7-В1 Методикой генерации псевдослучайных последовательностей для дальнейшего использования в криптографических алгоритмах
ОПК-3: Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями
Владеть:
ОПК-3-В1 Методикой анализа рисков информационной безопасности при построении системы защиты информации