

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Исаев Игорь Магомедович

Должность: Проректор по учебной работе

Дата подписания: 01.09.2023 14:08:47

Уникальный идентификатор документа:

d7a26b9e8ca85e98ec3de2eb454b4659d061f249

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

Промышленный интернет вещей и прогнозная аналитика

Квалификация

Магистр

Форма обучения

очная

Общая трудоемкость

5 ЗЕТ

Часов по учебному плану

180

Формы контроля в семестрах:

в том числе:

экзамен 1

аудиторные занятия

34

курсовая работа 1

самостоятельная работа

110

часов на контроль

36

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
	уп	рп	уп	рп
Неделя	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	Научно-исследовательская работа	
2.2.2	Управление функциональными задачами ИТ при реализации бизнес-процессов крупной компании	
2.2.3	Педагогическая практика	
2.2.4	Подготовка к процедуре защиты и защита выпускной квалификационной работы	

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-3-31	Методы защиты программного обеспечения от угроз информационной безопасности, методы защиты авторских прав на цифровой контент
ОПК-3-32	Основные методики анализа рисков информационной безопасности на предприятии
ОПК-3-33	Методы моделирования поведения нарушителя информационной безопасности. Принципы построения и функционирования сетей Петри
ОПК-1: Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	
Знать:	
ОПК-1-32	Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации
ОПК-1-31	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	
Уметь:	
ОПК-3-У2	Использовать концепцию управления рисками при анализе защищенности инфокоммуникационной структуры предприятия
ОПК-3-У5	Применять методы Парето-оптимизации в системе поддержки принятия решений в области проектирования системы защиты информации на предприятии
ОПК-3-У4	Моделировать поведение нарушителя с помощью сети Петри
ОПК-3-У3	Анализировать угрозы информационной безопасности и уязвимости систем защиты информации, строить модель информационной безопасности с полным перекрытием угроз
ОПК-1: Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте	
Уметь:	
ОПК-1-У2	Производить расчет критической длины линии связи при PNS-атаке на квантовый канал

ОПК-1-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
Владеть:
ОПК-3-В1 Методикой анализа рисков информационной безопасности при построении системы защиты информации
ОПК-1: Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте
Владеть:
ОПК-1-В1 Методикой генерации псевдослучайных последовательностей для дальнейшего использования в криптографических алгоритмах