

Документ подписан простой электронной подписью

Информационно-образовательное учреждение высшего образования
Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования

ФИО: Агабекян Раиса Левоновна

Должность: ректор «Академия маркетинга и социально-информационных технологий – ИМСИТ»

Дата подписания: 14.12.2023 08:54:15

(г. Краснодар)

Уникальный программный ключ:

(НАН ЧОУ ВО Академия ИМСИТ)

4237c7ccb9b9e111bbaf1f4fcd9201d015c4dbaa123ff774747307b9b9fbcbe

УТВЕРЖДАЮ

Проректор по учебной работе,

доцент Севрюгина Н.И.

20 ноября 2023

Б1.О.27

Методы и средства криптографической защиты информации

Аннотация к рабочей программе дисциплины (модуля)

Закреплена за кафедрой	Кафедра математики и вычислительной техники
Учебный план	10.03.01 Информационная безопасность
Квалификация	бакалавр
Форма обучения	очная
Программу составил(и):	к.ф.-м.н., доцент, Бужан Виталий Викорович

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	4 (2.2)		Итого	
	Неделя		16 1/6	
Вид занятий	уп	рп	уп	рп
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Контактная работа на аттестации	0,2	0,2	0,2	0,2
В том числе в форме практ.подготовки	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	48,2	48,2	48,2	48,2
Сам. работа	59,8	59,8	59,8	59,8
Итого	108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике.
1.2	
1.3	
1.4	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.О
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Основы информационной безопасности
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Сети и телекоммуникации
2.2.2	Безопасность компьютерных сетей
2.2.3	Защита информации от утечки по техническим каналам
2.2.4	Учебная практика: Учебно-лабораторная практика
2.2.5	Производственная практика: Технологическая практика
2.2.6	Выполнение и защита выпускной квалификационной работы
2.2.7	Производственная практика: Преддипломная практика
2.2.8	Производственная практика: Эксплуатационная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

Планируемые результаты обучения (показатели освоения индикаторов компетенций)

ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах

Знать:

Минимальный необходимый уровень знаний Использует средства криптографической защиты информации в автоматизированных системах

Уровень знаний Использует средства криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок

Уровень знаний Использует средства криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, без ошибок

ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов

Уметь:

Продемонстрированы основные умения Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме

Продемонстрированы все основные умения Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами

Продемонстрированы все основные умения Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме

ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации

Владеть:

Имеется минимальный набор навыков Организует защиту информации от утечки по техническим каналам на объектах информатизации с негрубыми ошибками и некоторыми недочётами

Продемонстрированы базовые навыки Организует защиту информации от утечки по техническим каналам на объектах информатизации с некоторыми недочётами

Продемонстрированы навыки Организует защиту информации от утечки по техническим каналам на объектах информатизации без ошибок и недочётов

ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации	
Знать:	
Минимальный необходимый уровень знаний Оценивает угрозы информационной безопасности объекта информатизации	
Уровень знаний Оценивает угрозы информационной безопасности объекта информатизации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок	
Уровень знаний Оценивает угрозы информационной безопасности объекта информатизации в объёме, соответствующем программе подготовки, без ошибок	
Уметь:	
Продемонстрированы основные умения Оценивает угрозы информационной безопасности объекта информатизации , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме	
Продемонстрированы все основные умения Оценивает угрозы информационной безопасности объекта информатизации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами	
Продемонстрированы все основные умения Оценивает угрозы информационной безопасности объекта информатизации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме	
Владеть:	
Имеется минимальный набор навыков Оценивает угрозы информационной безопасности объекта информатизации с негрубыми ошибками и некоторыми недочётами	
Продемонстрированы базовые навыки Оценивает угрозы информационной безопасности объекта информатизации с некоторыми недочётами	
Продемонстрированы навыки Оценивает угрозы информационной безопасности объекта информатизации без ошибок и недочётов	
ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
Знать:	
Минимальный необходимый уровень знаний Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
Уровень знаний Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок	
Уровень знаний Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации в объёме, соответствующем программе подготовки, без ошибок	
Уметь:	
Продемонстрированы основные умения Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме	
Продемонстрированы все основные умения Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами	
Продемонстрированы все основные умения Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме	
Владеть:	
Имеется минимальный набор навыков Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с негрубыми ошибками и некоторыми недочётами	
Продемонстрированы базовые навыки Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с некоторыми недочётами	
Продемонстрированы навыки Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации без ошибок и недочётов	

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
Минимальный необходимый уровень знаний Использует средства криптографической защиты информации в автоматизированных системах	
Минимальный необходимый уровень знаний Оценивает угрозы информационной безопасности объекта информатизации	
Минимальный необходимый уровень знаний Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
3.2	Уметь:
Продемонстрированы основные умения Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме	

Продемонстрированы основные умения Оценивает угрозы информационной безопасности объекта информатизации , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме	
Продемонстрированы основные умения Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме	
3.3	Владеть:
Имеется минимальный набор навыков Организует защиту информации от утечки по техническим каналам на объектах информатизации с негрубыми ошибками и некоторыми недочётами	
Имеется минимальный набор навыков Оценивает угрозы информационной безопасности объекта информатизации с негрубыми ошибками и некоторыми недочётами	
Имеется минимальный набор навыков Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с негрубыми ошибками и некоторыми недочётами	