

Документ подписан простой электронной подписью  
Информация о владельце:

ФИО: Макаренко Елена Николаевна

Должность: Ректор

Дата подписания: 24.04.2023 10:03:29

Уникальный программный ключ:

c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Закреплена за кафедрой

# Методы защиты от удаленных сетевых атак

Информационные технологии и защита информации

Учебный план 10.04.01.02\_1.plx

Форма обучения **очная**

## Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		Итого	
	Неделя			
Неделя	15 2/6			
Вид занятий	уп	рп	уп	рп
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Практические	32	32	32	32
Итого ауд.	80	80	80	80
Контактная работа	80	80	80	80
Сам. работа	28	28	28	28
Часы на контроль	36	36	36	36
Итого	144	144	144	144

## 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- 1.1 развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением защищенности информационных систем от удаленных сетевых атак; развитие профессиональных компетенций для нахождения оптимальных решений при построении защищенных информационных систем; привитие навыков использования специализированных средств защиты.

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

**УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий**

**ПК-4: Способен осуществлять анализ результатов экспериментальных исследований с применением математических и физических методов, выбор технических средств инструментального мониторинга защищенности объектов информатизации**

**В результате освоения дисциплины обучающийся должен:**

**Знать:**  
процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения.(соотнесено с индикатором УК-1.1.)  
формальные модели информационной безопасности объектов информатизации;основные характеристики и показатели эффективности средств и систем обеспечения информационной безопасности;  
источники и классификацию угроз информационной безопасности;основные характеристики технических средств обеспечения информационной безопасности от утечек по техническим каналам;  
методы обработки данных мониторинга информационной безопасности объектов информатизации;порядок создания и структуру отчета, создаваемого по результатам исследования (соотнесено с индикатором ПК-4.1.)

<b>Уметь:</b> принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий.(соотнесено с индикатором УК-1.2.) формализовать задачу обеспечения информационной безопасности объекта информатизации; анализировать и прогнозировать критерии эффективности обеспечения информационной безопасности объекта информатизации;классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, оценивать угрозы информационной безопасности;определять виды и типы технических средств обеспечения информационной безопасности; применять инструментальные средства мониторинга защищенности объекта информатизации;структурировать аналитическую информацию для включения в отчет(соотнесено с индикатором ПК-4.2.)
<b>Владеть:</b> методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения;методиками разработки стратегий действий при проблемных ситуациях.(соотнесено с индикатором УК-1.3.) навыками разработки модели информационной безопасности объекта информатизации; навыками определения класса защищенности информационных систем;навыками оценки критериев эффективности системы обеспечения информационной безопасности; навыками подготовки аналитических отчетов по результатам проведенного анализа (соотнесено с индикатором ПК-4.3.)