АННОТАЦИЯ

к рабочей программе дисциплины

«Анализ алгоритмов шифрования на наличие уязвимостей»

Составитель:

«Трифанов Александр Владимирович, аспирант каф. Метрологии и технологий оптического производства»

«Ф.И.О., степень, звание»

|  |  |
| --- | --- |
| Направление подготовки | 12.04.02 Оптотехника |
| Профиль подготовки | Компьютерная безопасность |
| Квалификация (степень) выпускника | магистр |
| Форма обучения | очная |
| Цикл, раздел учебного плана | Вариативная часть Б1.ДВ2.1 |
| Курс изучения | 2 |
| Количество зачетных единиц | 2 |
| Форма промежуточной аттестации | Зачет. |
| Количество часов всего, из них | 72 |
| - лекционные | 20 |
| - практические | 52 |
| - лабораторные | 0 |
| - СРС | 0 |
| - подготовка к экзамену | 0 |

1. Целями освоения дисциплины Анализ алгоритмов шифрования на наличие уязвимостейявляются формирование у студентов общекультурных, общепрофессиональных и профессиональных компетенций, определяющих их готовность и способность, как будущих специалистов по направлению подготовки «Оптотехника», к эффективному применению усвоенных знаний для поиска уязвимостей и их исправления в системах шифрования.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины:

общекультурные компетенции:

ОК-1 способностью к абстрактному мышлению, обобщению, анализу, систематизации и прогнозированию

ОК-3 способностью к саморазвитию, самореализации, использованию творческого потенциала

общепрофессиональные компетенции:

ОПК-2 способностью применять современные методы исследования, оценивать и представлять результаты выполненной работы

профессиональные компетенции:

ПК-103 способностью к проведению атак на компьютерные системы, системы защиты информации, системы предотвращения и обнаружения вторжений, системы антивирусной защиты и другие

ПК-104 способностью к оценке защищенности систем защиты, конфигурации сложных систем: анализ настроек и механизмов безопасности

3. Краткое содержание дисциплины

Раздел I. Введение  
Раздел II. Математические основы  
Раздел III. Формализация исходного кода алгоритмов шифрования  
Раздел IV. Методы анализа формальной записи алгоритмов шифрования  
Раздел V. Формальный анализ протоколов проверки подлинности и обмена ключами  
Раздел VI. Типы алгоритмов и криптографические режимы  
Раздел VII. Использование алгоритмов  
Раздел VIII. Специальные алгоритмы для протоколов

Аннотация разработана на основании ФГОС ВО по направлению подготовки магистров 12.04.02 Оптотехника от 28.11.2014 г.