АННОТАЦИЯ

к рабочей программе дисциплины

«Системы автоматического поиска и эксплуатации 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.В.7 |
| Курс изучения | 1 |
| Количество зачетных единиц | 4 |
| Форма промежуточной аттестации | Зачет. |
| Количество часов всего, из них | 144 |
| - лекционные | 20 |
| - практические | 96 |
| - лабораторные | 0 |
| - СРС | 28 |
| - подготовка к экзамену | 0 |

1. Целями освоения дисциплины Системы автоматического поиска и эксплуатации 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 применения систем автоматического поиска и эксплуатации уязвимостей и проведения оценки уровня защищенности исследумых систем.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины:

общекультурные компетенции:

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

общепрофессиональные компетенции:

ОПК-1 способностью формулировать цели и задачи исследования, выявлять приоритеты решения задач, выбирать и создавать критерии оценки

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

ОПК-3 способностью использовать иностранный язык в профессиональной сфере

профессиональные компетенции:

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

3. Краткое содержание дисциплины

Раздел I. Сканеры уязвимостей  
Раздел II. Инструмент для развётки эксплойтов Metasploit/Armitage  
Раздел III. Написание собственных модулей для Metasploit  
Раздел IV. Сканер Web уязвимостей ZAProxy  
Раздел V. Nessus  
Раздел VI. Использование sqlmap при поиске и эксплуатации SQL-инъекций  
Раздел VII. BBQSQL  
Раздел VIII. WAPT  
Раздел IX. Nikto  
Раздел X. Burp Suite  
Раздел XI. Protector Plus  
Раздел XII. MaxPatrol и XSpider 7

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