АННОТАЦИЯ

к рабочей программе дисциплины

«Обнаружение вторжений и мониторинг функционирования высокопроизводительных систем (включая системы обнаружения компьютерных атак)»

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.5 |
| Курс изучения | 2 |
| Количество зачетных единиц | 3 |
| Форма промежуточной аттестации | Экзамен. |
| Количество часов всего, из них | 108 |
| - лекционные | 10 |
| - практические | 62 |
| - лабораторные | 0 |
| - СРС | 0 |
| - подготовка к экзамену | 36 |

1. Целями освоения дисциплины Обнаружение вторжений и мониторинг функционирования высокопроизводительных систем (включая системы обнаружения компьютерных атак)являются 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 своевренного обнаружения и отражения вторжений в высокопроизводительные системы.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины:

общекультурные компетенции:

ОК-2 способностью действовать в нестандартных ситуациях, нести ответственность за принятые решения

общепрофессиональные компетенции:

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

профессиональные компетенции:

ПК-2 способностью к построению математических моделей объектов исследования и выбору численного метода их моделирования, разработке нового или выбор готового алгоритма решения задачи

ПК-101 способностью к разработке систем по анализу защищенности систем управления ресурсами предприятия: мониторинг настроек, анализ исходного кода, анализ бизнес-привилегий, описанию выявленных недостатков в корпоративных приложениях, обоснование угроз, составление рекомендаций и предложений по их устранению/предупреждению

ПК-102 проведение аналитических и статистических исследований программного обеспечения АСУ на предмет наличия уязвимостей, недекларированных возможностей, программных закладок

3. Краткое содержание дисциплины

Раздел I. Системы мониторинга Zabbix и Nagios  
Раздел II. Системы обнаружения вторжений (IDS)  
Раздел III. Аудит сетей с использованием Nsauditor Network Security Auditor  
Раздел IV. Использование KFSensor, для обнаружения вторжений  
Раздел V. Тестирование несанкционированных проникновений в систему с помощью программы Core Impact  
Раздел VI. Использование Snort для обнаружения и предотвращения вторжений  
Раздел VII. Изучение возможностей Linux Intrusion Detection System

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