Аннотация
к рабочей программе дисциплины
«Методы выявления нарушений информационной безопасности, аттестация автоматизированных систем»

по направлению 10.03.01 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 4 зачетных единиц.(144 часов)

Форма контроля: экзамен 8 семестр.

Предполагаемые семестры: 8

Цель изучение дисциплины (модуля) является овладение студентами методами выявления нарушений информационной безопасности.

Задачи курса:

- ознакомление с общими принципами работы традиционных механизмов защиты и систем обнаружения атак;
- изучение различных классификаций атак и уязвимостей;
- изучение перечня источников информации об атаках;
- ознакомление с методами обработки и анализа собранной информации об атаках;
- ознакомление с инфраструктурой обнаружения атак;
- ознакомление с проблемами, присущими технологии обнаружения атак и их решениями.

Учебная дисциплина относится к циклу Б1. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы технологии Cisco;
- сети и системы передачи информации;
- безопасность операционных систем;
- безопасность вычислительных сетей;
- английский язык в сфере профессиональных коммуникаций.

Знания и практические навыки, полученные в результате освоения дисциплины, используются студентами при разработке курсовых и дипломных работ, в научно-исследовательской работе.

Краткое содержание дисциплины:

Технология обнаружения атак, Выбор системы обнаружения атак, Система обнаружения атак RealSecure.

В результате изучения дисциплины, специалист должен обладать следующими профессиональными компетенциями (ПК):

ПК-6 Способностью принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;

ПК-7 Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

В результате изучения дисциплины бакалавр должен:

Знать:

– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

Уметь:

– формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
– осуществлять меры противодействия нарушениям сетевой безопасности с

использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности объекта;

Владеть:

- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- профессиональной терминологией в области информационной безопасности.