АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

ОЦЕНКА И КОНТРОЛЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(название дисциплины)

10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

2

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- «Оценка и контроль обеспечения информационной безопасности» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность». Целью освоения дисциплины является ознакомление магистров с администрированием безопасности информационных систем, с типовой структурой корпоративной информационной системы, с методиками управления безопасностью ИС, методах анализа и активного аудита безопасности такого класса систем, а также с типовыми защитными средствами в корпоративной информационно-вычислительной среде.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО (ВПО)

- Данная дисциплина относится к дисциплинам по выбору вариативной части блока Б1 (код Б1.В.ДВ.2). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.
- Дисциплина изучается на 1 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Корпоративные информационные системы» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: -информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; -фотоника, приборостроение, -оптические и биотехнические системы и технологии; -электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.
- Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Методы информационно-аналитической работы», «Защищённые информационные системы», «Организационно-правовые механизмы обеспечения информационной безопасности», «Управление информационной безопасностью» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен обладать:

- ПК-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации;
- ПК-10 – способностью проводить аттестацию объектов информатизации по требованиям безопасности информации.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Обнаружение узлов сети. icmp echo request.
- Обнаружение узлов сети средствами протокола tcp (tcp-ping).
- Обнаружение узлов сети средствами протокола arp (arp-ping).
- Дополнительные средства определения маршрутов ip-пакетов - nmap, tracemap, mrt, идентификация статуса tcp-портов (tcp-connect. syn-scan).
- Методы скрытого сканирования (stealth tcp scanning methods).
- Сканирование ip протокола. Идентификация прикладных служб. метод анализа стандартных приглашений (banner grabbing).

- Идентификация прикладных сетевых служб методом анализа особенностей реализации (smtp).
- Идентификация службы электронной почты.
- Активное исследование стека tcp/ip.

Составитель: доцент кафедры ИЗИ к.т.н., Монахов Ю.М.

должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов

ФИО, подпись

Директор института ИТР А.А. Галкин

ФИО, подпись

Дата, Печать института (факультета)