АННОТАЦИЯ

к рабочей программе дисциплины

«Операции и атаки в информационных системах и сетях»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Цель изучения дисциплины: является приобретение студентами знаний о структуре действий, предпринимаемые для достижения информационного превосходства в обеспечении национальной военной стратегии путем воздействия на информацию и информационные системы противника с одновременным укреплением и защитой собственной информации и информационных систем и инфраструктуры.

Задачи изучения дисциплины:

- сформировать у будущего специалиста в области безопасности телекоммуникационных систем знания, умения и навыки в области формализация описания информационных конфликтов социотехнических систем, стратегии и тактики информационных операций и атак, реализуемых в социотехнических системах. Стратегии реализации информационных операций и атак;

- предоставить возможность изучения технологии поиска и анализа следов информационных операций и атак и инцидентов, прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов.

Содержание дисциплины: Классификация по характеру воздействия; по цели воздействия; по наличию обратной связи с атакуемым объектом; по условию начала осуществления воздействия; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие. Примеры.

Сбор информации: изучение окружения; идентификация топологии сети; идентификация узлов; идентификация сервисов и сканирование портов; идентификация операционной системы; определение роли узла; определение уязвимостей узла; реализация атаки; проникновение; установление контроля; завершение атаки

Фрагментация данных; атака Ping flooding; нестандартные протоколы, инкапсулированные в IP; атака smurf; атака DNS spoofing; атака IP spoofing; навязывание пакетов; Sniffing — прослушивание канала; перехват

пакетов на маршрутизаторе; навязывание хосту ложного маршрута с помощью протокола ICMP; WinNuke; подмена доверенного хоста; отказ в обслуживании (DoS, DDoS-атаки):SYN-flood,UDP-flood

Методы анализа сетевой информации; статистический метод; экспертные системы; нейронные сети

Популярные фишинговые схемы: несуществующие ссылки; мошенничество с использованием брендов известных корпораций; подложные лотереи; ложные антивирусы и программы для обеспечения безопасности; IVR или телефонный фишинг. Сбор информации из открытых источников: плечевой серфинг; обратная социальная инженерия

Способы защиты от социальной инженерии. Классификация угроз: угрозы, связанные с телефоном; угрозы, связанные с электронной почтой; угрозы, связанные с использованием службы мгновенного обмена сообщениями. Основные защитные методы

Концепция «сетецентрических войн». Наступательные операции в киберпространстве как составная часть информационной войны. Наступательные операции против АСУ инфраструктурных и технологических объектов. Оборонительные операции как часть мер по обеспечению информационной безопасности в мирное время. Перспективы развития концепции кибернетических операций