АННОТАЦИЯ

к рабочей программе дисциплины

«Непосредственно и удаленно атакуемые компьютерные системы и сети»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Цель изучения дисциплины: приобретение будущими специалистами знаний и умений в части анализа угроз в отношении непосредственно и удалённо атакуемых информационной безопасности в компьютерных систем и сетей, участия в работах по управлению рисками систем защиты компьютерных систем и сетей от НСД.

Задачи изучения дисциплины:

- сформировать у будущего специалиста в области безопасности компьютерных систем и сетей знаний относительно классификации и этапов реализации атак, технологии обнаружения атак, в том числе в аспекте социальной инженерии;

- предоставить возможность изучения особенностей, проблем и перспектив применения кибернетического оружия в современной сетецентрической войне.

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

Перечень формируемых компетенций:

ПК-4.2 - Способен участвовать в проектировании программных и аппаратных средств защиты информации

ПК-4.1 - Способен определять угрозы безопасности, возможные источники и каналы утечки информации, а также принимать решения по обеспечению защиты информации, в том числе с использованием современных методов и программного инструментария искусственного интеллекта

Общая трудоемкость дисциплины: 5 з.е.

Форма итогового контроля по дисциплине: Зачет с оценкой