

АННОТАЦИЯ

к рабочей программе дисциплины

«Непосредственно и удаленно атакуемые кибернетические системы и сети»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

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 сетях электросвязи, участия в работах по управлению рисками систем защиты сетей электросвязи от НСД.

Задачи изучения дисциплины:

- сформировать у будущего специалиста в области безопасности телекоммуникационных систем 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 сетцентрической 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 «сетевых 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-9.5 - Способен принимать участие в обеспечении функционирования и разработке средств и систем защиты средств связи сетей электросвязи (СССЭ) от несанкционированного доступа (НСД)

Общая трудоемкость дисциплины: 4 з.е.

Форма итогового контроля по дисциплине: Зачет с оценкой