АННОТАЦИЯ

к рабочей программе дисциплины
«Мониторинг защищенности сетевой инфраструктуры телекоммуникационных систем»

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: является приобретение студентами знаний о методы контроля функционирования телекоммуникационных систем и сетей, принципах построения систем обнаружения компьютерных атак, методах обработки данных мониторинга безопасности телекоммуникационных систем и сетей

Задачи изучения дисциплины: сформировать у будущего специалиста в области безопасности телекоммуникационных систем знания, умения и навыки в области применения средств мониторинга работоспособности и эффективности применяемых средств защиты телекоммуникационных систем и сетей; применения инструментальных средств проведения мониторинга защищенности сетевых ресурсов телекоммуникационных систем и сетей, а также составления отчетов по результатам проверок защищенности телекоммуникационных систем и сетей

Содержание дисциплины

Корпоративная сеть как объект защиты

Событие безопасности. Понятие уязвимости. Классификация уязвимостей. Источники информации по уязвимостям Принятые обозначения уязвимостей. National Vulnerabllity Database. Уязвимости и безопасность промышленных систем управления

Обзор международных и российских стандартов, регламентирующих мониторинг безопасности. Принципы непрерывности.

Принципы и критерии выбора параметров мониторинга. Подходы к построению мониторинга. Мониторинг с участием агентов и мониторинг при помощи конечных агентов. Иерархии систем мониторинга. Протоколы мониторинга телекоммуникационных систем и сетей. Инструменты для осуществления мониторинга.

Разбор существующих систем мониторинга, их сильные и слабые стороны. Документальное оформление процедуры мониторинга. Описание инструкции реагирование на инциденты (плейбук). Организация мониторинга безопасности телекоммуникационных систем и сетей. IEEE 802.11i - нерешенные проблемы. Несанкционированное использование беспроводных устройств. Атаки на устройства и сервисы. Атаки на механизм аутентификации 802.1x. Атаки на клиентов. Мониторинг безопасности. Особенности обнаружения атак. Атаки, характерные для беспроводных сетей. Эксплойты и их разновидности. Использование техники запуска кода. Простые эксплойты. Удаленный подбор пароля. Оценка стойкости паролей. Тестирование. Анализ результатов. Отказ в обслуживании

Перечень формируемых компетенций:

ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности;

ОПК-9.3 - Способен проводить мониторинг защищенности сетевых ресурсов и формировать отчеты по выявленным уязвимостям

Общая трудоемкость дисциплины: 8 з.е.

Форма итогового контроля по дисциплине: Зачет с оценкой