АННОТАЦИЯ

к рабочей программе дисциплины

«Методическое обеспечение анализа защищенности информационных систем и сетей»

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: овладение принципами и методами организации процесса анализа защищенности автоматизированной системы и сетей.

Задачи изучения дисциплины:

- сформировать у студентов способность применения методов научных исследований при проведении разработок в области защиты информации в автоматизированных системах, в частности для процесса анализа защищенности автоматизированной системы и сетей

- способствование развитию навыков разработки методик и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.

Содержание дисицплины:

Проверки и оценки уровня ИБ организации. Оценка уязвимостей компьютерной системы. Разновидности проверок и оценок уровня ИБ организации. Рынок аналитических услуг в сфере ИБ. Место и роль аудита в модели обеспечения ИБ. Оценка уровня безопасности компьютерных систем: общие понятия и определения. Базовые определения. Принципы и формы аудита ИБ организации. Оценка уязвимостей компьютерной системы. Особенности автоматизированных информационных систем как объектов аудита ИБ. Исходная концептуальная схема (парадигма) проведения аудита ИБ.

Изучение исходных данных по АС; оценка рисков, связанных с наличием угроз безопасности в отношении ресурсов АС; анализ механизмов организационного уровня, политики; безопасности организации и организационно-распорядительной документации и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам; ручной анализ конфигурационных файлов маршрутизаторов, межсетевых экранов (МЭ) и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры; сканирование внешних сетевых адресов локальной вычислительной системы (ЛВС) из сети Интернет; сканирование ресурсов ЛВС изнутри; анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ. Стандарты проведения оценки уровня безопасности компьютерных систем

Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ. ISO 27001 (B 7799 - 2:2005). ISO 27002 (BS 7799 - 1:2005). Стандарты ISO/IEC и ГОСТ ИСО/МЭК 27005, BS 7799-3. Анализ рисков ИБ. Общие критерии (ГОСТ Р ИСО/МЭК 15408). Руководящие документы ФСТЭК России аудит в целях сертификации средств защиты и аттестации объектов нформатизации.Ста Банка России СТО БР ИББС- CoBit. Стандарт аудита PCI DSS. Соответствие и взаимодействие международного и российского подходов и методов аудита безопасности.

Стандарт аудита PCI DSS. Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ. Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ. Сбор свидетельств (исходной информации) для проведения аудита ИБ. Рекомендации по планированию аудита ИБ. Рекомендации по моделированию. Этапы проведения внутреннего и внешнего аудитов ИБ: общее и различия. Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование. Договор о проведении внешнего аудита ИБ. Порядок планирования аудита. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника. Методы сбора исходных данных: опрос, наблюдение, анализ. Методы анализа собранных свидетельств. Аудиторская группа: состав, права и обязанности, роли, привлечение технических специалистов. Обязанности проверяемой организации во время аудита ИБ.

Методы и инструментальные средства проведения аудита ИБ. Программные средства анализа и управления. Оценка уязвимостей компьютерной системы средствами Dallas Lock.

Инструментарий базового уровня - справочные и методические материалы. Инструментарий для обеспечения повышенного уровня безопасности. ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия. СОВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.

Перечень формируемых компетенций:

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах; ОПК-7.2. - Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;

Общая трудоемкость дисциплины: 9 з.е.

Форма итогового контроля по дисциплине: Зачет с оценкой