otus
онлайн-образование

Полная программа

Инфраструктура открытых ключей PKI

Инфраструктура открытых ключей PKI

Длительность курса: 88 часов

Модуль 1. Знакомство с криптографией

Тема 1
Защита информации, чем занимается криптография

Цель занятия
Изучить риски цифрового взаимодействия. Узнать какие виды атак на информацию существуют. Понять цели защиты информации и основные принципов работы криптографических алгоритмов.

Краткое содержание
Триада CIA, Гексад Паркера. Цели использования криптографии. Криптографические алгоритмы

Тема 2
История криптографии

Цель занятия
Изучить историю развития криптографии

Краткое содержание
Типовые методы защиты, применявшиеся до появления асимметричной криптографии

Тема 3
Алгоритм RSA. Принципы работы

Цель занятия
Изучить математические аспекты работы алгоритма RSA

Краткое содержание
Алгоритм RSA

Тема 4
Концепция доверия в IT инфраструктурах

Цель занятия
Познакомиться с концепцией доверия в ИТ инфраструктурах. Доверие и безопасность систем. Выяснить принципы построения доверия и к чему приводит потеря доверия, узнать что из себя представляет доверенная третья сторона.

Краткое содержание
Конфиденциальность информации, корректность использование информации, принципы реагирования при нарушении доверия, непрерывность доверия.

Тема 5
Идентификация, Аутентификация, Авторизация

Цель занятия
Познакомиться с терминологией. Понять систему законодательства РФ. Изучить элементы систем аутентификации и факторы аутентификации. Узнать принципы типовых атак. Узнать как работает аутентификация на основе асимметричной криптографии и какие варианты аутентификации обычно используются, их особенности.

Краткое содержание
NCSC-TG-017 - "A Guide to Understanding Identification and Authentication in Trusted Systems", Законодательство РФ в части идентификации, аутентификации, авторизации.

Домашние задания

Домашнее задание к модулю №1. Тест знаний основных теоретических вопросов модуля 1
Цель
Проверка полученных теоретических знаний

Модуль 2. Цифровые сертификаты открытого ключа, шифрование и электронная подпись, проектирование PKI

Тема 1
Сертификаты открытого ключа и списки отзывов сертификатов

Цель занятия
Понять цели использования сертификатов открытого ключа. Изучить структуру сертификата открытого ключа (стандарт X.509). Понять как работает Удостоверяющий центр Познакомиться со списками отзыва сертификатов и методами их распространения. Изучить жизненный цикл сертификатов открытого ключа.

Краткое содержание
Стандарты X.509, RFC 5280, RFC 6818.

Тема 2
Знакомство с типами алгоритмов шифрования, Электронный документооборот и электронная подпись

Цель занятия
Разобраться с принципами работы основных криптографических алгоритмов, и узнать для чего они используются.

Краткое содержание
Симметричные и асимметричные алгоритмы шифрования, хеширование, цифровая подпись. Принципы построения электронного документооборота

Тема 3
Проектирование архитектуры PKI

Цель занятия
Изучить теоретические основ построения инфраструктуры открытых ключей

Краткое содержание
Основы проектирования инфраструктуры открытых ключей на основе решений Microsoft

Тема 4
Выбор среды виртуализации и создание виртуальных машин. Что предваряет развертывание PKI. Подготовка инфраструктурных сервисов

Цель занятия
Познакомиться со средами виртуализации. Подготовить собственный виртуальный стенд.

Краткое содержание
VMWare Workstation, Fusion. Oracle VirtualBox

Тема 5
Политика безопасности PKI и способы ее реализации

Цель занятия
Понять принципы обеспечения безопасности инфраструктуры открытых ключей

Краткое содержание
Теоретические основы обеспечения безопасности PKI. Microsoft Certificate Service Windows Server 2019/2022

Домашние задания

Домашнее задание к модулю №2. Проектирование инфраструктуры открытого ключа. Решение предложенного преподавателем бизнес-кейса. Подготовить виртуальный стенд для проведения лабораторных работ.
Цель
Получен навык проектирования инфраструктуры открытых ключей с учетом всех особенностей изучаемой организации. Подготовлен виртуальный стенд.

Модуль 3. Установка и настройка удостоверяющих центров

Тема 1
Синтаксис файла capolicy.inf. Установка корневого УЦ и его пост. установочная настройка. Развертывание издающего УЦ и его пост. установочная настройка. Центры распространения сертификатов УЦ и списков отзыва сертификатов

Цель занятия
Понять структуру, функций и целей использования и синтаксис файла capolicy.inf. Получить навык развертывания и настройки УЦ Microsoft Certificate Service. Настроить центры распространения сертификатов и списков отзыва.

Краткое содержание
Microsoft Certificate Service Windows Server 2019/2022

Тема 2
Online Certificate Status Protocol - цели использования и внедрение. Сервис web Enrollment

Цель занятия
Изучить протокола OCSP

Краткое содержание
Microsoft Certificate Service. Протокол OCSP. Windows Server 2019/2022

Домашние задания

Домашнее задание к модулю №3. Установка и настройка УЦ
Цель
Подготовит файлы capolicy.inf для предварительной настройки УЦ. Подготовит скрипты для развертывания и настройки УЦ. Выполнит установку и настройку двухуровневой иерархии УЦ. Получены навыки развертывания PKI для тестовой компании

Модуль 4. Обеспечение отказоустойчивости и высокой доступности PKI

Тема 1
Иерархии УЦ, кластеризация и дублирование. Отказоустойчивость точек распространения. Балансировка нагрузки

Цель занятия
Узнать как обеспечить отказоустойчивость и высокую доступность инфраструктуры открытых ключей на основе Microsoft Certificate Service. Построить отказоустойчивое решение для центров распространения. Изучить принципы балансировки нагрузки для решений PKI.

Краткое содержание
Microsoft Certificate Service. Microsoft Cluster Server. Windows Server 2019/2022. Технологии NLB.

Домашние задания

Домашнее задание к модулю №4. Тест знаний основных теоретических вопросов модуля 4
Цель
Проверка полученных теоретических знаний

Модуль 5. Управление PKI

Тема 1
Резервное копирование и восстановление

Цель занятия
Изучить как осуществлять резервного копирования и восстановления инфраструктуры открытых ключей Microsoft и сопутствующих сервисов

Краткое содержание
Microsoft Certificate Service. Системы резервного копирования. System State. Реестр Windows Server

Тема 2
Настройка разделения ролей и проверка работоспособности ролевой модели

Цель занятия
Изучить цели и принципы построения ролевой модели Microsoft Certificate Service

Краткое содержание
Microsoft Certificate Service. Windows Server 2019/2022. GPO

Тема 3
Шаблоны сертификатов, роль и цели использования, назначение полномочий на шаблоны сертификатов

Цель занятия
Познакомиться с шаблонами сертификатов, их структурой и целями использования. Разобраться с назначением полномочий на шаблоны сертификатов. Узнать какие риски безопасности возникают при неправильном назначении полномочий на шаблоны сертификатов

Краткое содержание
Microsoft Certificate Service. Windows Server 2019/2022

Домашние задания

Домашнее задание к модулю №5. Резервное копирование и восстановление инфраструктуры открытых ключей предприятия. Работа с шаблонами сертификатов. Настройка строгой ролевой модели.
Цель
Навыки резервного копирования и восстановления системы. Настройка шаблонов сертификатов и назначение полномочий на шаблоны сертификатов. Создание и проверка ролевой модели разделения полномочий.

Модуль 6. Практика применения PKI

Тема 1
Шифрование, EFS и BitLocker. Внедрение EFS в корпоративной среде

Цель занятия
Узнать принципы обеспечения шифрования хранимых данных на серверах Microsoft Windows

Краткое содержание
Windows Server 2019/2022, Microsoft Certificate Service. EFS. BitLocker

Тема 2
Безопасность информационного обмена (SSL/TLS). Внедрение SSL/TLS в корпоративной среде

Цель занятия
Изучить как обеспечивается безопасная передачи данных по общедоступным сетям

Краткое содержание
Протокол TLS

Тема 3
Внедрение безопасной электронной почты в корпоративной среде

Цель занятия
Изучить как обеспечивается безопасный обмен почтовыми сообщениями

Краткое содержание
Windows Server 2019/2022, Microsoft Certificate Service

Тема 4
Внедрение двухфакторной аутентификации на основе асимметричной криптографии смарт-карт и USB-ключей в корпоративной среде. Управление жизненным циклом средств аутентификации

Цель занятия
Разобраться с особенностями двухфакторной аутентификации на основе асимметричной криптографии смарт-карт и USB-ключей в корпоративной среде. Понять как выполняется управление жизненным циклом средств аутентификации.

Краткое содержание
Windows Server 2019/2022, Microsoft Certificate Service. EFS, Aladdin JaCarta Management System

Домашние задания

Домашнее задание к модулю №6. Тест знаний основных теоретических вопросов модуля 6
Цель
Проверка полученных теоретических знаний

Модуль 7. Проектная работа

Тема 1
Выбор темы и организация проектной работы

Цель занятия
выбрать и обсудить тему проектной работы;
спланировать работу над проектом.

Краткое содержание
правила работы над проектом и специфика проведения итоговой защиты; требования к результату проекта и итоговой документации.

Домашние задания

Проектная работа

Тема 2
Защита проектных работ

Цель занятия
защитить проект и получить рекомендации экспертов.

Краткое содержание
презентация проектов перед комиссией; вопросы и комментарии по проектам.

Тема 3
Подведение итогов курса

Цель занятия
узнать, как получить сертификат об окончании курса, как взаимодействовать после окончания курса с OTUS и преподавателями, какие вакансии и позиции есть для выпускников (опционально - в России и за рубежом) и на какие компании стоит обратить внимание

Краткое содержание
организационные вопросы;
рынок вакансий по направлению; статистика курса и вопросы по курсу.

Тема 4
Консультация по проектам и домашним заданиям