OTUS
онлайн-образование

Полная программа

Защита данных от утечек. DLP-системы

Защита данных от утечек. DLP-системы

Длительность курса: 138 часов

Модуль 1. Вводная часть. Знакомство с курсом

Тема 1
Вводный урок. Актуальность защиты информации от утечек

Цель занятия
обсудить какие цели преследует обучение на курсе, какие темы будут рассмотрены;
обсудить что необходимо для успешного прохождения курса.

Краткое содержание
концепция и цель курса;
знакомство с командой преподавателей;
общий обзор курса;
необходимое ПО для прохождения курса;
введение в защиту информации;
актуальность защиты информации.

Тема 2
Основная терминология ИБ

Цель занятия
разобраться в основных терминах и определениях, используемых в информационной безопасности;
ориентироваться в основных методологиях, используемых организацией для предотвращения утечки данных;
рассмотреть законодательство в области защиты информации от утечек;
обсудить для чего разрабатывается модель угроз безопасности информации в организации.

Краткое содержание
основные определения ИБ (защищаемая информация, безопасность информации, данные, утечка информации);
законодательство в области защиты информации от утечек (ПДн, коммерческая тайна, тайна связи);
модель угроз безопасности информации;
основные методологии ИБ.

Тема 3
Угрозы безопасности информации. Внутренний нарушитель // ДЗ

Цель занятия
обсудить какие существуют угрозы безопасности информации;
обсудить каким образом и зачем ведется мониторинг активности сотрудников;
обсудить почему необходимо проводить подготовку и тренинги сотрудников в области ИБ;
разработать модель нарушителя.

Краткое содержание
виды угроз безопасности информации;
внутренние и внешние угрозы, актуальность внутренних угроз;
умышленные и непреднамеренные угрозы;
модель угроз внутреннего нарушителя;
мониторинг активности сотрудников (employee monitoring, UAM, UEBA);
осведомленность, подготовка, контроль работы и тренинги сотрудников.

Домашние задания

Разработать модели нарушителя безопасности информации
Цель
Разработать модель нарушителя безопасности информации.

Тренируемые навыки:
- умение определять какие могут быть внутренние и внешние нарушители;
- умение разрабатывать модель нарушителя безопасности информации в компании.

Модуль 2. Защита информации от утечек

Тема 1
Общие аспекты защиты информации от утечек

Цель занятия
обсудить какие существуют источники утечки информации, их классификацию;
обсудить какие существуют особенности утечки информации в зависимости от источника;
обсудить каким образом предотвращать утечку информации.

Краткое содержание
общие аспекты защиты информации от утечек;
особенности утечки информации;
меры защиты информации от утечек.

Тема 2
Источники утечки информации // ДЗ

Цель занятия
обсудить какие есть виды и каналы источников утечки информации;
обсудить как происходит утечка информации при эксплуатации вычислительных систем;
обсудить как сотрудники могут стать источником утечки информации.

Краткое содержание
классификация каналов утечки информации (человек, аппаратура, программа);
виды источников утечки информации;
непреднамеренные каналы утечки информации;
утечка информации при эксплуатации вычислительных систем;
источники утечки информации в вычислительных системах (энергозависимые ЗУ, ОЗУ, файловые серверы, RAID);
сотрудники как источники утечки информации;
технические каналы утечки информации.

Домашние задания

Определить возможные источники утечки информации в рассматриваемой компании
Цель
Определить возможные источники утечки информации в рассматриваемой компании.

Тренируемые навыки:
- умение определять каналы атаки и источники возможной утечки информации;
- умение описать ресурсы компании, которые могут быть подвержены утечке и возможные последствия от утечки информации.

Тема 3
Каналы утечки информации

Цель занятия
обсудить какие существуют технические каналы утечки информации и их характеристику и классификацию;
обсудить как происходит утечка информации по техническим каналам;
обсудить как выстроить защиту информации от утечки по техническим каналам.

Краткое содержание
характеристики технических каналов утечки информации;
классификация технических каналов утечки информации;
способы утечки информации по техническим каналам;
защита информации от утечки по техническим каналам.

Тема 4
Технические каналы утечки информации // ДЗ

Цель занятия
обсудить какими способами можно организовать защиту информации от утечки;
рассмотреть требования законодательства в области защиты информации.

Краткое содержание
виды способов защиты информации от утечки;
организационные способы защиты информации от утечки;
законодательство, определяющее защиту информации от утечки.

Домашние задания

Разработать регламента по защите информации от утечки
Цель
Разработать регламент по защите информации от утечки в рассматриваемой компании.

Тренируемые навыки:
- умение определять правила работы с данными для сотрудников, исходя из их должностей;
- умение разрабатывать инструкцию структурным подразделениям по защите информации;
- умение определять обязанности сотрудников по защите информации от утечки.

Тема 5
Предотвращение утечки информации // ДЗ

Цель занятия
обсудить каким образом можно организовать защиту информации от утечки, какие для этого использовать средства.

Краткое содержание
обеспечение безопасности рабочих мест, физическая защита информации (защита от проникновения (контроль доступа в помещения - двери, окна, усиленные стены, охранные устройства, биометрические средства защиты);
организация защиты информации от утечки с использованием технических средств;
организация защиты информации от утечки с использованием программно-аппаратных и программных средств защиты

Домашние задания

Разработать модели угроз безопасности информации
Цель
Разработать модель угроз безопасности информации в рассматриваемой компании.

Тренируемые навыки:
- умение определять угрозы безопасности информации (возможные утечки) в рассматриваемой компании;
- умение обосновать требования безопасности информации (по предотвращению от утечек).

Модуль 3. Решения DLP

Тема 1
Общие сведения о DLP

Цель занятия
обсудить как работает DLP система ее архитектуру и классификацию;
использовать принцип и режимы работы DLP-системы.

Краткое содержание
что такое DLP система?
основные функции DLP;
принцип и режимы работы DLP;
архитектура DLP-систем;
классификация и виды (хостовые, шлюзовые) DLP.

Тема 2
Задачи, выполняемые DLP-системами // ДЗ

Цель занятия
обсудить какие задачи решает DLP система;
обсудить какие существуют технические возможности получения информации с использованием DLP систем;
обсудить какие существуют виды перехвата информации с помощью DLP систем.

Краткое содержание
основные задачи, решаемые DLP;
технические возможности получения информации;
перехват, мониторинг и анализ траффика (виды перехвата информации).

Домашние задания

Провести анализ перехваченного трафика
Цель
Провести анализ перехваченного трафика.

Тренируемые навыки:
- уменеие осуществлять перехват трафика
- умение анализировать перехваченный трафик
- умение выявлять признаки утечки информации

Тема 3
Компоненты DLP-систем и их взаимодействие

Цель занятия
обсудить как работают компоненты централизованного управления DLP-системы;
обсудить как работают компоненты сетевого уровня DLP-системы;
обсудить как работают компоненты уровня хоста DLP-системы.

Краткое содержание
компоненты централизованного управления;
компоненты сетевого уровня;
компоненты уровня хоста.

Тема 4
Обзор зарубежных DLP-систем

Цель занятия
обсудить какие существуют DLP решения на мировом рынке, в чем их отличия;
обсудить каким образом и зачем необходимо реализовывать импортозамещение DLP в организации.

Краткое содержание
RSA Data Loss Prevention Suite;
Symantec DLP Suite;
McAfee DLP;
Forcepoint DLP;
импортозамещение в условиях современных реалий.

Тема 5
Российские DLP-системы

Цель занятия
обсудить какие существуют российские DLP системы в чем их отличия;
обсудить каким образом и зачем необходимо реализовывать импортозамещение DLP в организации.

Краткое содержание
Infowatch Traffic Monitor;
Стахановец;
Search Inform;Solar Dozor - «Ростелеком-Солар»;
StaffCop - ООО «Атом Безопасность»;
DeviceLock DLP;
Falcongaze SecureTower;
Zecurion DLP;
Гарда Предприятие;
КИБ СёрчИнформ.

Тема 6
Международное и российское законодательство в области DLP

Цель занятия
рассмотреть нормативные документы в области применения DLP;
обсудить как законно, не нарушая прав и вобод работников внедрить DLP в организации.

Краткое содержание
как DLP может нарушать права и свободы работников (неприкосновенность частной жизни);
легитимность применения DLP;
нормативные документы регуляторов в области применения DLP;
юридические аспекты применения DLP (сертификат ФСТЭК);
обеспечение законного внедрения DLP.

Тема 7
Внедрение DLP-систем в организации // ДЗ

Цель занятия
рассмотреть какие этапы внедрения DLP-систем в организации;
подготовить организацию к внедрению DLP системы.

Краткое содержание
этапы внедрения;
подготовка к внедрению (разработка документации, юридическое обоснование, выбор решения);
проектирование;
схема внедрения;
установка и настройка;
интеграция с другими системами.

Домашние задания

Разработать план внедрения DLP в организации
Цель
Разработать план внедрения DLP в организации.

Тренируемые навыки:
- умение подготовить информационную инфраструктуру к внедрению DLP;
- умение планировать внедрение DLP в организации.

Модуль 4. Практическая работа с системой DLP

Тема 1
Подготовка и установка DLP – системы // ДЗ

Цель занятия
подготовиться к установке DLP-системы в организации;
устанавить и оптимизировать DLP систему после установки.

Краткое содержание
подготовка к установке;
выбор способа установки;
установка и оптимизация.

Домашние задания

Разворачивание DLP системы
Цель
Произвести установку DLP системы.

Тренируемые навыки:
- умение производить установку DLP системы;
- уметь производить запускать и проверять работоспособность DLP системы.

Тема 2
Первичная настройка DLP – системы // ДЗ

Цель занятия
создать и настроить базу данных DLP системы;
производить настройку основных конфигураций DLP системы;
создать базовые шаблоны в DLP системе.

Краткое содержание
настройка базы данных;
настройка основных функций и конфигураций;
создание базовых шаблонов (классификаторов).

Домашние задания

Создание базы данных и первичная настройка DLP системы
Цель
Тренируемые навыки:
- создание и насройка базы данных, необходимой для работоспособности DLP системы;
- умение производить первичную настройку DLP системы.

Тема 3
Настройка прав доступа // ДЗ

Цель занятия
настроить права доступа с использованием DLP системы;
настроить DLP систему на блокирование нежелательного контента;
настроить запрет и разрешение устройств с использованием DLP системы.

Краткое содержание
настройка групповых прав;
настройка прав пользователей;
настройка разрешенных устройств;
блокирование нежелательного контента.

Домашние задания

Настройка прав доступа, создание белого и черного списка устройств
Цель
Тренируемые навыки:
- умение настраивать прав доступа пользователей с помощью DLP;
- создание белого и черного списка устройств.

Тема 4
Настройка политик безопасности данных: создание и настройка правил // ДЗ

Цель занятия
настроить запрет нелегитимного копирования на внешние носители информации;
настроить ограничения на отправку файлов по электронной почте;
настроить загрузку файлов в облачное хранилище и обратно.

Краткое содержание
настройка копирования на внешние носители (запрет нелегитимного копирования);
настройка передачи сообщений электронной почты;
настройка передачи информации из облачного хранилища;
результаты работы политики (блокирование, уведомление).

Домашние задания

Настройка объектов защиты
Цель
Тренируемые навыки:
- настройка правил копирования на внешние носители;
- настройка отправки файлов по электронной почте;
- настройка загрузки и выгрузки из облачного хранилища.

Тема 5
Настройка политик безопасности данных: действия при срабатывании правил // ДЗ

Цель занятия
создать и настроить правила DLP системы;
настроить действия при срабатывании правил;

Краткое содержание
создание и настройка правил;
настройка действий при срабатывании правил;
результаты работы политики.

Домашние задания

Создание и настройка правил DLP-системы
Цель
Тренируемые навыки:
- умение создавать шаблоны правил DLP-системы;
- умение производить настройку срабатывания правил DLP-системы.

Тема 6
Интеграция DLP с другими системами // ДЗ

Цель занятия
обсудить с какими системами может интегрироваться DLP;
интегрировать DLP с другими системами.

Краткое содержание
интеграция с SIEM и САВЗ;
интеграция с IdM (Identity Management), IAM (Identity and Access Management), IGA (Identity Governance & Administration);
интеграция с SOAR (Security Orchestration, Automation and Response) и DRM (Digital Rights Management);
интеграция с LDAP (Active Directory).

Домашние задания

Интеграция DLP со средством защиты информации
Цель
Уметь интегрировать DLP с другими системами.

Тренируемые навыки:
- уметь интегрировать DLP с Active Directory;
- уметь интегрировать DLP с прокси-сервером по ICAP.

Тема 7
Анализ перехваченных данных // ДЗ

Цель занятия
провести анализ цепочек событий с использованием DLP системы;
провести копирайтный анализ с использованием DLP системы;
провести поведенческий анализ сотрудников с использованием DLP системы.

Краткое содержание
анализ цепочек событий;
копирайтный анализ;
поведенческий анализ сотрудников.

Домашние задания

Проведение анализа данных с использованием DLP системы
Цель
Тренируемые навыки:
- умение проводить контентный анализ с использованием DLP системы;
- умение проводить контекстный анализ с использованием DLP системы;
- умение проводить анализ с использованием регулярных выражений;
- умение проводить лексический анализ с использованием DLP системы.

Тема 8
Подготовка к проведению расследования инцидентов // ДЗ

Цель занятия
определить источник утечки информации с использованием DLP;
собрать информацию и доказательства о нарушении.

Краткое содержание
проверка и выявление нарушения;
определение источника утечки информации с использованием DLP;
определение критичности инцидента;
сбор и фиксация доказательств.

Домашние задания

Обнаружение источника утечки информации с использованием DLP
Цель
Тренируемые навыки:
- умение выявлять источник утечки с использованием DLP;
- умение собирать доказательства утечки информации с использованием DLP.

Тема 9
Проведение расследования инцидентов // ДЗ

Цель занятия
уметь проводить внутреннее расследование инцидентов с использованием DLP;
уметь оформлять отчетную документацию по проведенному расследованию.

Краткое содержание
оформление внутренней документации (служебная записка, приказ о внутреннем расследовании, комиссия по расследованию, сбор объяснений сотрудников,)
проведение внутреннего расследования инцидентов с применением DLP.

Домашние задания

Проведение расследования компьютерного инцидента с использованием DLP
Цель
Тренируемые навыки:
- умение проводить анализ отчетов по данным журнала аудита;
- умение проводить анализ отчетов по данным журнала теневого копирования.

Тема 10
Формирование отчетов с использованием DLP // ДЗ

Цель занятия
сформировать отчеты по результатам расследования инцидентов с использованием DLP систем;
разработать документацию по результатам расследования инцидентов.

Краткое содержание
формирование списков инцидентов;
формирование таблиц;
формирование диаграмм;
официальное оформление доказательств.

Домашние задания

Формирование отчета по проведенному расследованию компьютерного инцидента
Цель
Тренируемые навыки:
- умение создавать, обновлять, экспортировать с сохранать отчеты DLP системы;
- умение написать отчет по проведенному расследованию инцидента с применением DLP системы.

Модуль 5. Проектная работа

Тема 1
Выбор темы и организация проектной работы // Проект

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

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

Домашние задания

Проектная работа
Цель
Закрепить и продемонстрировать полученных знаний и навыков.

Тема 2
Консультация по проектам и домашним заданиям

Цель занятия
получить ответы на вопросы по проекту, ДЗ и по курсу.

Краткое содержание
вопросы по улучшению и оптимизации работы над проектом;
затруднения при выполнении ДЗ;
вопросы по программе.

Тема 3
Защита проектных работ

Цель занятия
защитить проект и получить рекомендации экспертов.

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

Тема 4
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;
проведение собеседований;
статистика курса и вопросы по курсу.