Полная программа

Информационная безопасность. Basic

Информационная безопасность. Basic

Длительность курса: 116 часов

Модуль 1. Правовая база и основы обеспечения ИБ

Тема 1
Введение. Знакомство с курсом. Систематизация понятий

Цель занятия

ориентироваться в структуре курса, применять основные термины в области ИБ.

Краткое содержание

знакомство;
карта компетенций;
организация процесса и результаты обучения;
мотивация;
лайфхаки;
актуальность темы;
систематизация понятий ИБ: защита информации, информационная и кибер- безопасность, объект защиты, уязвимость, угроза, риск и другие.

Тема 2
Система нормативных правовых актов в области ИБ, органы обеспечения информационной безопасности и защиты информации

Цель занятия

ориентироваться в основных нормативных правовых актах и регулирующих органах в области ЗИ и ИБ;
знать механизмы регулирования ИБ.

Краткое содержание

механизмы государственного регулирования: лицензирование, аккредитация, сертификация и аттестация;
основные регуляторы в области ИБ и ЗИ, их полномочия;
основные сведения о ФСТЭК России, полномочия в части лицензирования и оценки соответствия.

Тема 3
Основы обеспечения безопасности сведений конфиденциального характера

Цель занятия

ориентироваться в основных нормативных актах, относящих сведения к категории ограниченного доступа;
знать основные шаги по обеспечению безопасности сведений конфиденциального характера в организации.

Краткое содержание

информация, обладатель информации и доступа к информации, информационная система, несанкционированный доступ, предоставление, распространение, разглашение и утечки информации, общедоступная информация и ограниченный доступ;
права и обязанности обладателя информации;
перечень сведений конфиденциального характера и основные нормативные акты, относящие сведения к категории ограниченного доступа;
шаги по обеспечению безопасности сведений конфиденциального характера, примеры.

Тема 4
Основы обеспечения безопасности критической информационной инфраструктуры (КИИ)

Цель занятия

знать проблематику, основные принципы и подходы к обеспечению безопасности КИИ;
ориентироваться в нормативных документах в области безопасности КИИ.

Краткое содержание

основные понятия в области безопасности КИИ;
проблематика, основные принципы и подходы к обеспечению безопасности КИИ;
система нормативных документов в области безопасности КИИ.

Тема 5
Стандарты и лучшие практики в области ИБ. Основы управления ИБ

Цель занятия

ориентироваться в стандартах и лучших практиках в области ИБ, принципах управления ИБ, основах создания защищаемых систем.

Краткое содержание

основы национальной, региональной и международной стандартизации;
примеры и источники стандартов и лучших практик в области ИБ;
основные принципы управления ИБ;
основы создания защищенных систем.

Тема 6
Анализ рисков и моделирование угроз // ДЗ

Цель занятия

ориентироваться в основных понятиях и деятельности по управлению рисками;
описывать угрозы безопасности информации.

Краткое содержание

основные понятия и цели деятельности по анализу рисков и моделированию угроз безопасности информации;
использование Методики оценки угроз безопасности информации ФСТЭК России и БДУ ФСТЭК России при описании угроз, популярные модели и методики анализа (оценки) рисков.

Домашние задания

Построение модели угроз безопасности информации

Цель

описать угрозы безопасности информациии по предложенной преподавателем методике.

Тема 7
Ответственность за правонарушения и преступления в области ИБ

Цель занятия

ориентироваться в основных видах юридической ответственности и последствиях за правонарушения в области ИБ.

Краткое содержание

основные понятия и виды юридической ответственности;
характер правонарушений (преступлений) о области ИБ;
примеры правонарушений (преступлений) и их последствий.

Тема 8
Групповая менторская консультация

Цель занятия

получить ответы на вопросы по ДЗ;
получить ответы на вопросы по пройденным темам.

Краткое содержание

ответы на вопросы и обсуждение ошибок при выполнении ДЗ.

Модуль 2. Способы и средства обеспечения ИБ на современном ландшафте угроз

Тема 1
Современный ландшафт угроз, способы и средства обеспечения ИБ // ДЗ

Цель занятия

ориентироваться в современных угрозах и тенденциях изменения ландшафта угроз ИБ;
выбирать способы и средства противодействия угрозам.

Краткое содержание

современные угрозы ИБ;
тенденции изменения ландшафта угроз ИБ;
способы и средства противодействия угрозам.

Домашние задания

Развернуть виртуальную машину под управлением Kali Linux

Цель

Овладеть навыками установки операционной системы Kali Linux, освоить основные функции фильтрации трафика в программе Wireshark, ознакомиться с базовыми методами сканирования портов на целевом хосте.

Тема 2
Основы криптографической защиты информации (КЗИ)

Цель занятия

применять основные термины в области криптографической защиты информации (КЗИ);
ориентироваться в методах и средствах КЗИ.

Краткое содержание

основные понятия в области КЗИ и в сфере электронной подписи (ЭП); история, методы, алгоритмы КЗИ;
отечественные криптографические стандарты; инфраструктура открытых ключей (PKI), ФЗ "Об электронной подписи", виды ЭП и сертификатов ключа проверки ЭП, удостоверяющий центр (УЦ) и его функции.

Тема 3
Вопросы эксплуатации средств криптографической защиты информации (СКЗИ) // ДЗ

Цель занятия

ориентироваться в СКЗИ;
понимать, как выбирать СКЗИ под решаемые задачи.

Краткое содержание

примеры применения криптографических методов для решения задач обеспечения безопасности информации и участников информационного взаимодействия;
лицензирование и сертификация в области СКЗИ, классы СКЗИ;
выбор СКЗИ под решаемые задачи;
порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации, с использованием сертифицированных СКЗИ; примеры сертифицированных СКЗИ и особенности их применения.

Домашние задания

Учет СКЗИ

Цель

учесть СКЗИ при получении и установке на АРМ пользователя

Тема 4
Основы безопасности ОС // ДЗ

Цель занятия

ориентироваться в основных механизмах безопасности современных ОС.

Краткое содержание

архитектура безопасности и её особенности для ОС Windows и Linux: роли, привилегии, управление доступом;
стек технологий: Windows, Linux.

Домашние задания

Настройка SELinux

Цель

Настроить веб-сервер Apache в безопасной конфигурации с использованием механизма SELinux, обеспечив его корректную работу с учётом политик принудительного контроля доступа.

Тема 5
Групповая менторская консультация

Цель занятия

получить ответы на вопросы по ДЗ;
получить ответы на вопросы по пройденным темам.

Краткое содержание

ответы на вопросы и обсуждение ошибок при выполнении ДЗ.

Тема 6
Механизмы безопасности сертифицированной ФСТЭК версии ОС Linux // ДЗ

Цель занятия

выполнять настройку основных механизмов безопасности сертифицированной ФСТЭК версии ОС Linux.

Краткое содержание

настройка основных механизмов безопасности на примере одной из популярных сертифицированных ФСТЭК версий Linux (Астра/Ред/Альт): в том числе идентификации и аутентификации, дискреционного и мандатного механизмов управления доступом, средств ограничения программной среды и других.

Домашние задания

Настройка ограничений на вход пользователей в систему

Цель

создать учетные записи пользователей и настроить ограничения по входу в систему.

Тема 7
Основы антивирусной защиты. Поиск и удаление вредоносного ПО. Reverse-engineering. Анализ программ на вредоносность

Цель занятия

проверять ОС Windows на наличие следов инфицирования вредоносным ПО;
ориентироваться в методах проведения экспресс-анализа ПО на наличие вредоносного кода.

Краткое содержание

основы антивирусной защиты;
проверка ОС Windows на наличие следов инфицирования вредоносным ПО;
методы очистки системы от вредоносного ПО;
превентивные средства противодействию заражению; методы проведения экспресс-анализа ПО на наличие вредоносного кода;
Стек технологий: sysinternals suite, политики безопасности Windows, black/white lists; динамический анализ кода, настройка cuckoo sandbox, volatility.

Тема 8
Reverse-engineering. Ошибки реализации и написание эксплоитов

Цель занятия

ориентироваться в уязвимостях приложений;
знать принципы разработки эксплоитов для них.

Краткое содержание

разбор примеров уязвимостей в приложениях и способов их эксплуатации.

Тема 9
DevSecOps

Цель занятия

ориентироваться в методологии непрерывной безопасной разработки.

Краткое содержание

безопасная разработка приложений;
место и роль безопасности в DevOps.

Тема 10
Безопасность конечных устройств

Цель занятия

ориентироваться в основных уязвимостях и угрозах для конечных устройств;
выбирать методы и средства защиты конечных устройств.

Краткое содержание

уязвимости и угрозы для конечных устройств;
методы и средства защиты и поддерживающие технологии.

Тема 11
Основы сетевой безопасности

Цель занятия

ориентироваться в основных угрозах и атаках на вычислительные сети.

Краткое содержание

ландшафт сетевой безопасности;
как нужно защищать все типы сетей;
типы инструментов атаки, которые используют злоумышленники;
сетевые атаки разведки, доступа и социальной инженерии.

Тема 12
Безопасность облачных систем

Цель занятия

ориентироваться в основных угрозах для облачных систем;
выбирать методы и средства защиты облачных систем.

Краткое содержание

основные угрозы, методы и средства защиты облачных систем;
стек технологий: XaaS.

Тема 13
Безопасность веб-приложений

Цель занятия

анализировать строение современного веб-приложения;
понимать влияние его компонентов на безопасность.

Краткое содержание

понятие веб-приложения;
приложения, построенные на сложной инфраструктуре (балансировщики, кэши);
исследование безопасности исходного кода;
стек технологий: NGINX, Spring, Tomcat, Java, PHP

Тема 14
Комплексная кибербезопасность компании

Цель занятия

выбирать решения для обеспечения комплексной кибербезопасности компании и эффективно их комбинировать.

Краткое содержание

актуальные решения для обеспечения комплексной кибербезопасности компаний;
эффективное использование доступных инструментов.

Тема 15
Особенности обеспечения безопасности автоматизированных систем управления технологическими процессами (АСУ ТП)

Цель занятия

ориентироваться в особенностях обеспечения безопасности АСУ ТП, методах и средствах защиты АСУ ТП;
выбирать средства защиты АСУ ТП.

Краткое содержание

основная терминология;
примеры АСУ ТП в различных отраслях;
примеры атак на АСУ ТП;
методы и средства обеспечения безопасности АСУ ТП.

Тема 16
Групповая менторская консультация

Цель занятия

получить ответы на вопросы по ДЗ;
получить ответы на вопросы по пройденным темам.

Краткое содержание

ответы на вопросы и обсуждение ошибок при выполнении ДЗ.

Модуль 3. Обеспечение ИБ при эксплуатации защищаемых информационных систем

Тема 1
Эксплуатация и контроль защищенных систем // ДЗ

Цель занятия

ориентироваться в типовых ролях и задачах деятельности по эксплуатации и контролю защищаемых ИС (АС);
планировать деятельность по эксплуатации и контролю защищаемых ИС (АС).

Краткое содержание

жизненный цикл защищаемых ИС (АС);
примеры систем, ролей и функций персонала в них;
общие подходы по обеспечению ИБ при формировании и назначении ролей персонала защищаемых систем;
особенности допуска персонала защищаемой системы к работе;
типовые задачи и функции персонала при эксплуатации и выводе из эксплуатации защищаемых систем;
виды, примеры контроля и деятельности по контролю защищаемых систем.

Домашние задания

Разработка инструкции

Цель

В этом ДЗ вам нужно создать инструкцию пользователя по обращению с СКЗИ.

Тема 2
Мониторинг событий безопасности. Средства управления событиями информационной безопасности

Цель занятия

ориентироваться в средствах управления событиями и информацией о информационной безопасности.

Краткое содержание

обзор решений для мониторинга событий безопасности класса SIEM.

Тема 3
Контроль привилегированных пользователей

Цель занятия

знать методы и средства контроля привилегированных пользователей.

Краткое содержание

особенности управления привилегированным доступом;
выявление действий внутренних нарушителей, включая администраторов с помощью решений PAM, EDR, взаимодействия с SIEM.

Тема 4
Основы тестирования на проникновение. Атаки на сеть. Противодействие реагированию

Цель занятия

ориентироваться в методах атак;
оценивать защищенность;
знать виды, этапы и инструменты пентеста;
ориентироваться в типовых атаках и способах обхода средств обнаружения и реагирования.

Краткое содержание

методы атак;
мотивы злоумышленников;
методы оценки защищенности;
пентест и его виды;
этапы проведения пентеста/атак, матрица MITRE;
основные инструменты пентеста на каждом из этапов;
обзор ресурсов для тренировки навыков;
типовые атаки на сетевую инфраструктуру;
средства обнаружения и реагирования, и как злоумышленники пытаются их обходить.

Тема 5
Тестирование на проникновение. Поиск уязвимостей в операционной системе

Цель занятия

ориентироваться в основных типах уязвимостей для ОС.

Краткое содержание

подходы к поиску уязвимостей;
бинарные и логические уязвимости; уязвимости инфраструктуры под управлением Windows AD;
Стек технологий: Windows, Linux, MacOS, ProcMon, strace, LDAP, KERBEROS, Powershell.

Тема 6
Тестирование на проникновение для веб-приложений

Цель занятия

ориентироваться в основных уязвимостях и подходах к тестированию на проникновение для веб-приложений.

Краткое содержание

методики поиска уязвимостей
OWASP TOP 10;
CWE TOP 25;
WSTG;
стек технологий: языки программирования для веб; Burp Suite; nuclei project.

Тема 7
Основы деятельности по реагированию на инциденты ИБ

Цель занятия

знать в этапах деятельности по реагированию на инциденты ИБ.

Краткое содержание

подготовка к реагированию на инциденты ИБ;
обнаружение и регистрация инцидентов;
информирование об инцидентах;
локализация, выявление и устранение последствий;
закрытие инцидентов информационной безопасности;
анализ, установление причин и расследование инцидентов;
определение улучшений для системы информационной безопасности организации.

Тема 8
Исследование и описание артефактов скомпрометированной системы

Цель занятия

ориентироваться в основных действиях, выполняемых в ходе расследования инцидентов.

Краткое содержание

поиск артефактов, анализ файловой системы и оперативной памяти.

Тема 9
Расследование инцидентов. Анализ продвижения по сети

Цель занятия

знать основные методы продвижения злоумышленника по информационным системам организации;
знать методы обнаружения такого продвижения.

Краткое содержание

основные методы продвижения злоумышленника по информационным системам организации;
методы обнаружения такого продвижения;
стек технологий: SMB; запланированные задания; WMI/WRM.

Тема 10
Групповая менторская консультация

Цель занятия

получить ответы на вопросы по ДЗ;
получить ответы на вопросы по пройденным темам.

Краткое содержание

ответы на вопросы и обсуждение ошибок при выполнении ДЗ.

Модуль 4. Проектная работа

Тема 1
Выбор темы и организация проектной работы

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

Исследование в области информационной безопасности

Цель

закрепление пройденного на курсе материала по выбранной теме

Тема 2
Карьерная консультация

Цель занятия

узнать о направлениях и дальнейшем карьерном развитии для специалиста по информационной безопасности.

Краткое содержание

карьерные маршруты.

Тема 3
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 4
Защита проектных работ. Подведение итогов курса

Цель занятия

защитить проект и получить рекомендации экспертов.

Краткое содержание

презентация проектов перед комиссией;
вопросы и комментарии по проектам.