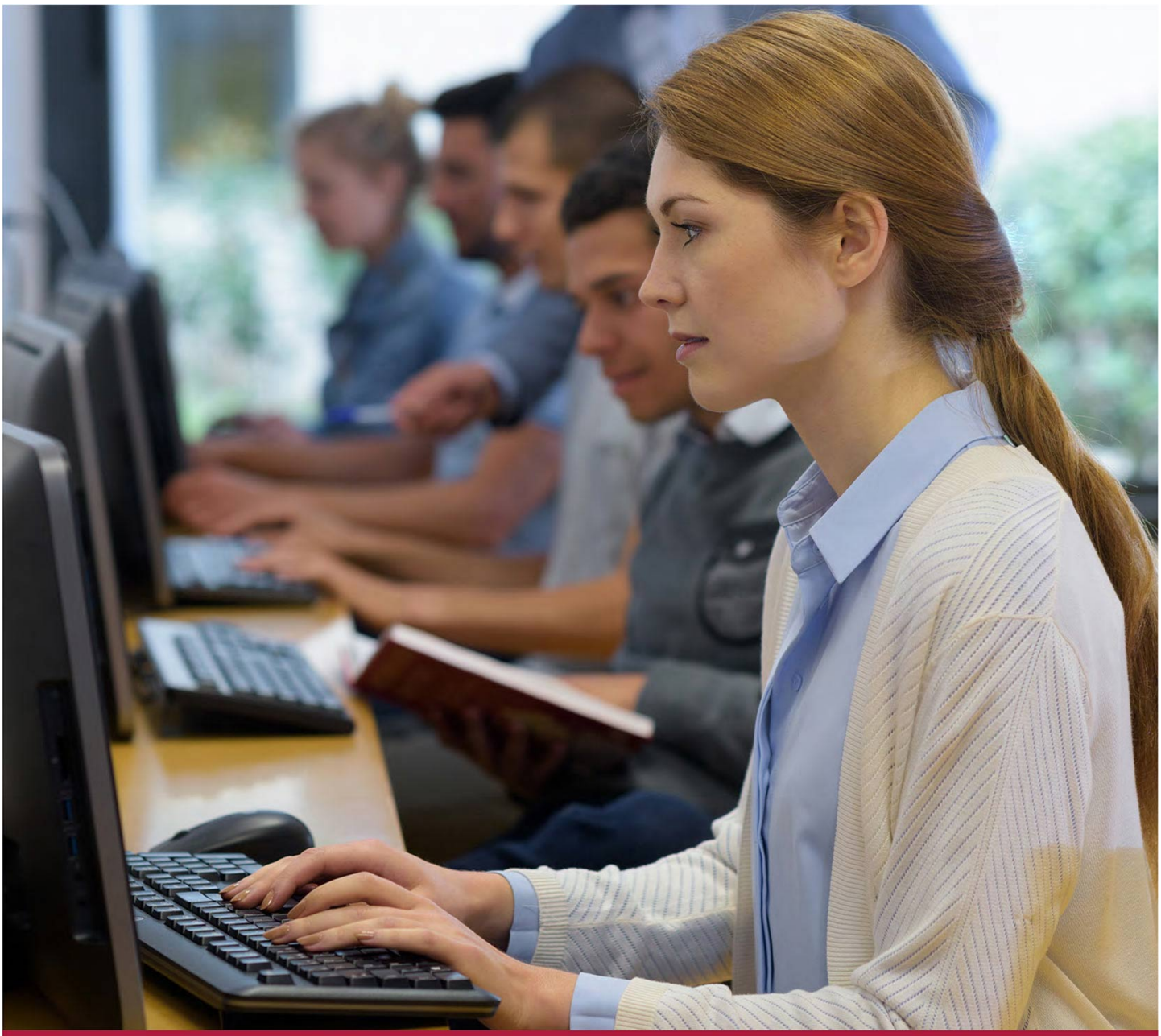
Академия АйТи
a Softline Company



Информационная безопасность. Обеспечение безопасности компьютерных систем и сетей.

Код курса: ИБ400

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Информационная безопасность. Обеспечение безопасности компьютерных систем и сетей.

Код курса: ИБ400

Длительность	400 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Специалист в области информационной кибербезопасности - актуальная и востребованная профессия в настоящее время. Растет количество инцидентов, наиболее атакуемыми отраслями стали информационные технологии, промышленность и ритейл. Выросла доля компьютерных атак — они составили 78% от общего количества; для организаций самые распространенные последствия кибератак - утечки конфиденциальной информации и нарушение основной деятельности, наблюдается большое количество утечек персональных данных пользователей, массовые атаки через эксплуатации уязвимостей. Последствия атак носят разнообразный характер: успешные кибератаки затрагивают предприятия и малого, и крупного бизнеса. Специалисты по обеспечению безопасности компьютерных систем и сетей принимают непосредственное участие в создании защиты информации, ее аудите и мониторинге, анализируют информационные риски, разрабатывают и внедряют мероприятия по предотвращению кражи информации. В компетенции также входит установка, настройка и сопровождение технических средств защиты информации. Курс Правительства РФ направлен на использование российского ПО, отечественных облачных решений, используемых на значимых объектах критической информационной инфраструктуры, планируется полное импортозамещение в таких сегментах софта, как серверное и связующее ПО, СУБД, средства виртуализации, мониторинга и управления, а также операционные системы и системы контейнеризации.

Подробная информация

Программа повышения квалификации разработана на основании:

- профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Приказом Минтруда России от 14 сентября 2022 г. № 533н;
- профессионального стандарта «Специалист по технической защите информации», утвержденного Приказом Минтруда России от 09 августа 2022 г. № 474н;
- ФГОС высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденного Приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1459;
- ФГОС высшего образования по направлению 10.03.01 Информационная безопасность (уровень

бакалавриата), утвержденного Приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427

Успешное окончание обучения по программе позволит специалистам:

- применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;
- организовывать защиту информации ограниченного доступа в компьютерных системах и сетях;
- применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;
- решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;
- проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;
- применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;
- принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

Успешное окончание обучения по программе позволит специалистам владеть навыками:

- работы с действующей нормативной правовой и методической базой в области организационного и правового обеспечения информационной безопасности;
- проверки состояния организации работ и выполнения требований по защите информации от несанкционированного доступа;
- установки и настройки программных (программно-технических) средств защиты информации от несанкционированного доступа;
- технического обслуживания программно-технических средств защиты информации от несанкционированного доступа;
- обнаружения и исправления ошибок в программных средствах защиты информации от несанкционированного доступа;
- устранения неисправностей и организации ремонта программно-технических средств защиты информации от несанкционированного доступа;
- подготовки отчетных материалов по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий;
- определения состава применяемых программно-аппаратных средств защиты информации в операционных системах и компьютерных сетях;
- разработки порядка применения программно-аппаратных средств защиты информации в операционных системах;
- установки программно-аппаратных средств защиты информации в операционных системах и компьютерных сетях;
- конфигурирования программно-аппаратных средств защиты информации в операционных системах;
- контроля корректности функционирования программно-аппаратных средств защиты информации в операционных системах;

- управления антивирусной защитой операционных систем в соответствии с действующими требованиями;
- настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации;
- управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях;
- контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях;
- управления средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями;
- определения порядка установки программного обеспечения с целью соблюдения требований по защите информации;
- контроля за соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение;
- формулирования требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения;
- выполнения работ по обнаружению вредоносного программного обеспечения;
- ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования;
- формулирования требований к встроенным средствам защиты информации программного обеспечения;
- оценки работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик;
- оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик;
- определения уровня защищенности и доверия программно-аппаратных средств защиты и формирования политик безопасности компьютерных систем;
- консультирования по вопросам безопасности компьютерных систем;
- разработки технических заданий на создание средств защиты информации;
- определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети;
- разработки модели угроз безопасности информации;
- задания требований к защите информации компьютерной системы;
- разработки руководящих документов по защите информации в организации;
- формулирования предложений по устранению выявленных уязвимостей компьютерных систем и сетей.

Целью реализации программы является формирование компетенций, необходимых специалистам для обеспечения информационной безопасности предприятия (организации) и защиты компьютерных систем и сетей.

Целевая аудитория:

- Специалисты по компьютерным сетям
- Системные администраторы
- Специалисты-техники по компьютерным сетям и системам
- Программисты

Необходимая подготовка: Уровень образования лица, поступающих на обучение – высшее или

среднее профессиональное в области информатики, вычислительной техники и информационных технологий.

Программа курса

Модуль 1. Нормативное правовое и методическое обеспечение технической защиты информации

Тема 1.1 Актуальность проблемы обеспечения информационной безопасности, основные понятия и термины

Тема 1.2 Система нормативного правового и методического обеспечения защиты информации

Тема 1.3 Угрозы информационной безопасности

Тема 1.4 Ответственность за нарушение требований по защите информации

Модуль 2. Техническая защита конфиденциальной информации

Тема 2.1 Организация защиты конфиденциальной информации на объектах информатизации

Тема 2.2 Проектирование систем защиты конфиденциальной информации

Тема 2.3 Техническая защита конфиденциальной информации от специальных воздействий

Тема 2.4 Контроль состояния технической защиты конфиденциальной информации

Модуль 3. Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей

Тема 3.1 Документы, определяющие требования к средствам защиты от НСД

Тема 3.2 Профили защиты

Тема 3.3 Требования по защите компьютерных систем и сетей

Тема 3.4 Формирование политики безопасности

Тема 3.5 Установка и настройка СЗИ от НСД

Тема 3.6 Установка и настройка СЗИ и резервного копирования

Модуль 4. Безопасность операционной системы Linux

Тема 4.1 Уровни информационной безопасности

Тема 4.2 Дискреционный контроль доступа к файлам

Тема 4.3 Linux Security Modules (LSM)

Тема 4.4 Штатные средства усиления защиты системы

Тема 4.5 Виртуализация как инструмент защиты

Тема 4.6 Дополнительные инструменты защиты

Модуль 5. Технологии построения защищенных компьютерных сетей

Тема 5.1 Технологии трансляции IP-адресов

Тема 5.2 Технологии межсетевых экранов

Тема 5.3 Системы обнаружения вторжений (СОВ/IDS)

Тема 5.4 Прокси-серверы

Тема 5.5 Сегментация локальной сети

Тема 5.6 Безопасная конфигурация и управление VPN

Тема 5.7 Защита беспроводных сетей

Тема 5.8 Использование UTM-решений для защиты сети

Модуль 6. Анализ защищенности компьютерных систем и сетей

Тема 6.1 Нормативно-правовые акты, регламентирующие процесс анализа защищенности

Тема 6.2 Аттестационные испытания

Тема 6.3 Система анализа уровня защищенности

Тема 6.4 Аналитический отчет по результатам проведенного анализа уровня защищенности

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru