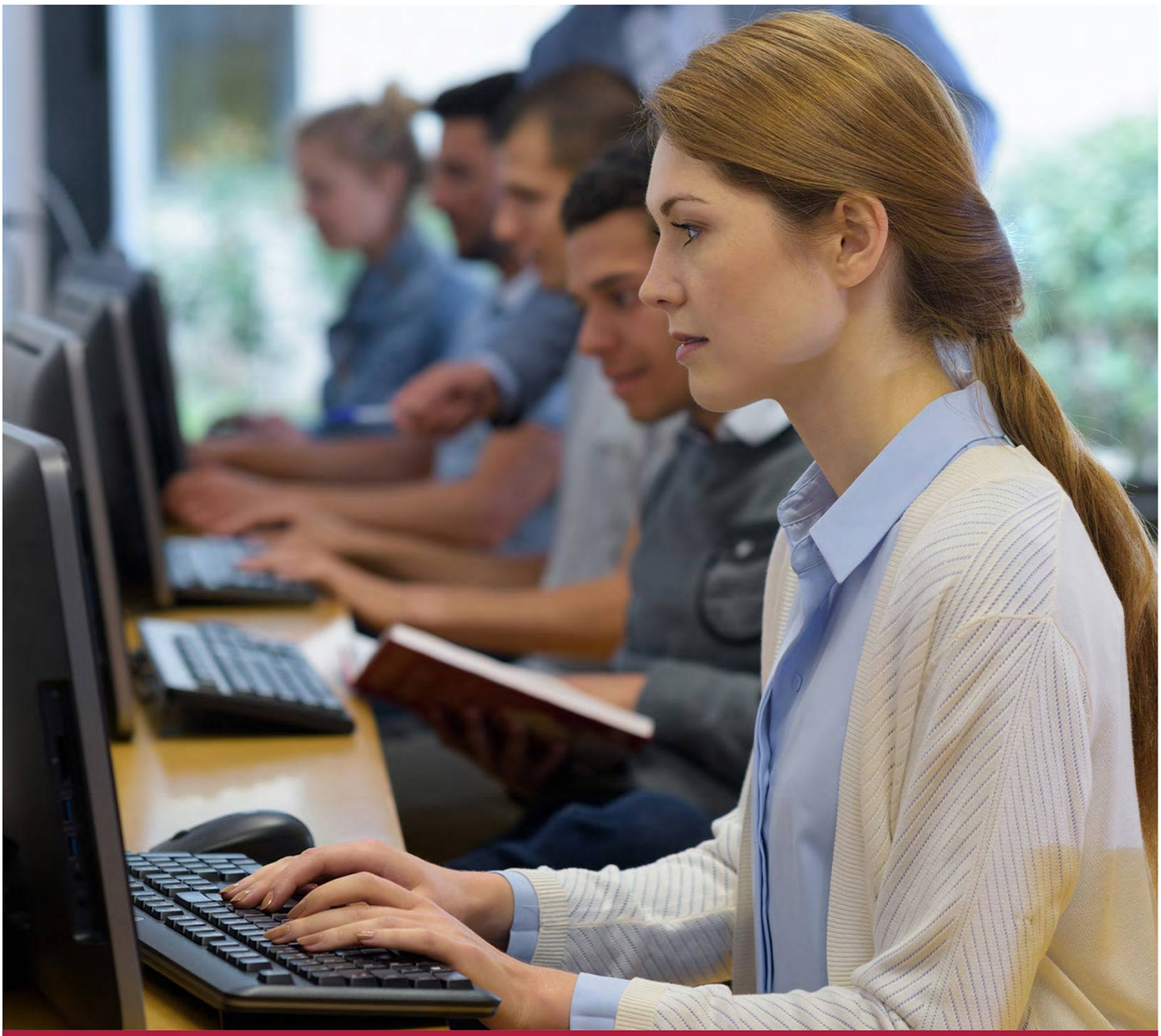
Академия АйТи
a Softline Company



Кибербезопасность для топ-менеджеров

Код курса: MK_TOP_IB

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

Кибербезопасность для топ-менеджеров

Код курса: MK_TOP_IB

Длительность	8 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс разработан специально для руководителей высшего звена, как имеющих опыт работы в области информационной безопасности, так и не имеющих профильной подготовки. Основное внимание уделяется построению и управлению системой обеспечения информационной безопасности (ИБ) в организации, соблюдению законодательства в сфере защиты объектов критической информационной инфраструктуры (КИИ), реагированию на компьютерные инциденты и атаки, а также выполнению нормативных требований по защите персональных данных. Курс помогает руководителям выработать комплексное понимание ИБ и ее стратегического значения для защиты компании от современных киберугроз и правовых рисков.

Подробная информация

Профиль аудитории:

Руководители и сотрудники, ответственные за обеспечение информационной безопасности в организации.

Предварительные требования:

- базовые знания в области компьютерных систем и сетей;
- навыки работы с операционными системами, электронной почтой, сетью Интернет.

По окончании курса слушатели смогут:

- Эффективно управлять системой информационной безопасности в организации. Понимать принципы и методики построения системы ИБ, организацию работы с рисками и разработку комплексных стратегий защиты.
- Понимать требования законодательства по защите объектов КИИ. Создавать системы безопасности объектов КИИ в соответствии с федеральным законодательством и нормативными требованиями.
- Организовывать процесс реагирования на компьютерные инциденты и атаки. Понимать роль организации в системе ГосСОПКА, строить внутренние процессы по ликвидации последствий компьютерных атак и восстановлению работы после инцидентов.

- Обеспечивать соответствие нормативным требованиям по защите персональных данных. Разрабатывать и поддерживать процессы информационной безопасности в информационных системах персональных данных.
- Понимать административную и уголовную ответственность за нарушения в области ИБ. Выявлять возможные риски и предупреждать нарушения, тем самым снижая угрозы правовых санкций для компании.

Программа курса

Модуль 1: Система обеспечения информационной безопасности в организации

- **Особенности деятельности по защите информации:** риск-ориентированный подход к обеспечению информационной безопасности.
- **Государственная система обеспечения информационной безопасности:** роль государства в сфере информационной безопасности, регуляторы и их функции.
- **Построение корпоративной системы ИБ**: основные компоненты, политика информационной безопасности, требования к специалистам, требования к средствам обеспечения информационной безопасности.
- **Организационная структура ИБ**: взаимодействие отделов и распределение ответственности, роль высшего руководства.
- **Лицензирование деятельности по защите информации**: федеральный закон, лицензирование деятельности по ТЗКИ, лицензирование деятельности по криптографической защите информации.

Модуль 2: Законодательство по обеспечению безопасности объектов критической информационной инфраструктуры (КИИ)

- **Основные требования российского законодательства**: федеральный закон и подзаконные нормативные акты.
- **Значимые объекты КИИ**: порядок категорирования объектов КИИ.
- **Построение системы безопасности для значимых объектов КИИ**: требования к созданию системы безопасности значимых объектов КИИ.
- **Обязанности организации как субъекта КИИ**: проведение категорирования, обеспечения безопасности значимых объектов КИИ, вопросы импортозамещения ПО и ПАК, взаимодействие с регулирующими органами (ФСТЭК, ФСБ), указ Президента №250 от 01.05.2022.

Модуль 3: Компьютерные инциденты и атаки, реагирование и роль организации

- **Понятие компьютерного инцидента и атаки**: различия между инцидентом и атакой, типы компьютерных атак и их признаки, примеры компьютерных инцидентов на объектах КИИ и реагирования на них.
- **ГосСОПКА**: функции и состав государственной системы обнаружения, предупреждения и ликвидации компьютерных атак (ФЗ №187, Указ Президента РФ №31).
- **Роль организации в системе ГосСОПКА**: обязанности по выявлению и реагированию на компьютерные атаки, взаимодействие с НКЦКИ, Роскомнадзором и ФСБ.
- **Алгоритм реагирования на инциденты**: действия по ликвидации последствий, восстановление нормальной работы системы, внутреннее расследование и отчетность.
- **Управление инцидентами на уровне руководства**: процесс принятия решений при

инцидентах.

Модуль 4: Нормативные требования к защите персональных данных

- **Законодательство о защите персональных данных**: ФЗ №152 «О персональных данных» и иные нормативные акты.
- **Требования к информационным системам**: уровни защищенности ИСПДн, требования к защите персональных данных, разработка и утверждение локальных актов.
- **Процессы обработки и защиты персональных данных в организации**: сбор, хранение, передача (распространение, предоставление, доступ) и уничтожение персональных данных.
- **Контроль соблюдения требований законодательства в сфере персональных данных**: внутренний аудит, взаимодействие с Роскомнадзором и субъектами персональных данных.

Модуль 5: Ответственность за нарушение требований ИБ

- **Административная ответственность**: виды правонарушений в сфере ИБ, штрафные санкции и другие меры ответственности согласно КоАП РФ.
- **Уголовная ответственность**: преступления, связанные с неисполнением или нарушением требований ИБ, соответствующие статьи УК РФ.
- **Судебная практика в сфере персональных данных**: обзор типовых правонарушений и преступлений, связанных с нарушениями в области персональных данных.
- **Роль руководителя в предотвращении нарушений**: контроль за соблюдением законодательства, повышение осведомленности персонала.

Заключение

- Подведение итогов: ключевые выводы по каждому модулю.
- Вопросы и ответы.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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