



Академия АйТи  
a Softline Company



## Основы информационной безопасности: принципы и обнаружение атак

Код курса: ОИБ-01

# Основы информационной безопасности: принципы и обнаружение атак

Код курса: ОИБ-01

<b>Длительность</b>	40 ак. часов
<b>Формат</b>	
<b>Разработчик курса</b>	Академия АйТи
<b>Тип</b>	Учебный курс
<b>Способ обучения</b>	Под руководством тренера

## О курсе

Комплексный вводный курс, предназначенный для руководителей и сотрудников, отвечающих за внедрение и осуществление контроля за политикой информационной безопасности на предприятии. Курс применяется для формирования базовых и прикладных компетенций в области принципов информационной безопасности, понимания современных угроз и моделей атак, а также освоения подходов и средств обнаружения атак и инцидентов безопасности в автоматизированных системах и корпоративных сетях. В рамках курса под руководством инструктора рассматриваются фундаментальные понятия и модели угроз информационной безопасности, архитектура и принципы функционирования средств обнаружения атак, а также роль этих средств в системе обеспечения информационной безопасности организации. Существенное внимание уделяется признакам атак, источникам данных о событиях безопасности, методам их анализа и корреляции.

## Подробная информация

### Профиль аудитории:

- Курс будет интересен конечным пользователям, которым требуются знания в области информационной безопасности, для понимания и соответствия правилам, определенным в политике информационной безопасности предприятия.
- Курс можно рекомендовать работникам кадровых, юридических, технических и других департаментов, вовлеченных в разработку политики информационной безопасности.
- Начинающим специалистам в сфере Информационной безопасности

### Предварительные требования:

- Базовые знания в области компьютерных систем и сетей.
- Навыки работы с сетевыми операционными системами, электронной почтой, сетью Интернет.

### По окончании курса слушатели изучат:

- Формирование политики безопасности, в соответствии с требованиями компании;
- Процесс подготовки соответствующих пакетов документов;
- Средства для защиты информации от несанкционированного доступа;

- Средства для безопасной работы в сети.
- Механизмы реагирования на события безопасности;
- Методы поиска признаков атак в различных источниках.

## Программа курса

### Модуль 1 «Введение в информационную безопасность»

- Понятие информации и информационной безопасности
- Угрозы, нарушитель, риски информационной безопасности
- Государственная система обеспечения

### Модуль 2 «Правовые аспекты обеспечения безопасности информации»

- Законодательство РФ в области информации и ИБ
- Правовое регулирование обработки персональных данных
- Коммерческая тайна и конфиденциальная информация
- Ответственность за нарушения в сфере ИБ

### Модуль 3 «Средства защиты информации от несанкционированного доступа»

- Идентификация, аутентификация и управление доступом
- Контроль целостности и аудит безопасности

### Модуль 4 «Обеспечение безопасности компьютерных систем и сетей»

- Угрозы сетевой безопасности
- Межсетевые экраны и VPN
- IDS/IPS и ловушки

### Модуль 5 «Система обеспечения информационной безопасности в организации»

- Принципы построения СОИБ
- Политика ИБ и регламентирующие документы
- Управление рисками и инцидентами

### Модуль 6 «Обнаружение атак»

- Обнаружение атак как механизм защиты
- Терминология: события, атаки, уязвимости, инциденты
- Источники данных для обнаружения атак
- Признаки атак
- Методы обнаружения атак
- Механизмы реагирования и анализ результатов

[Посмотреть расписание курса и записаться на обучение](#)

**Обращайтесь по любым вопросам**

к менеджерам Академии АйТи

**+7 (495) 150 96 00** | [academy@academyit.ru](mailto:academy@academyit.ru)