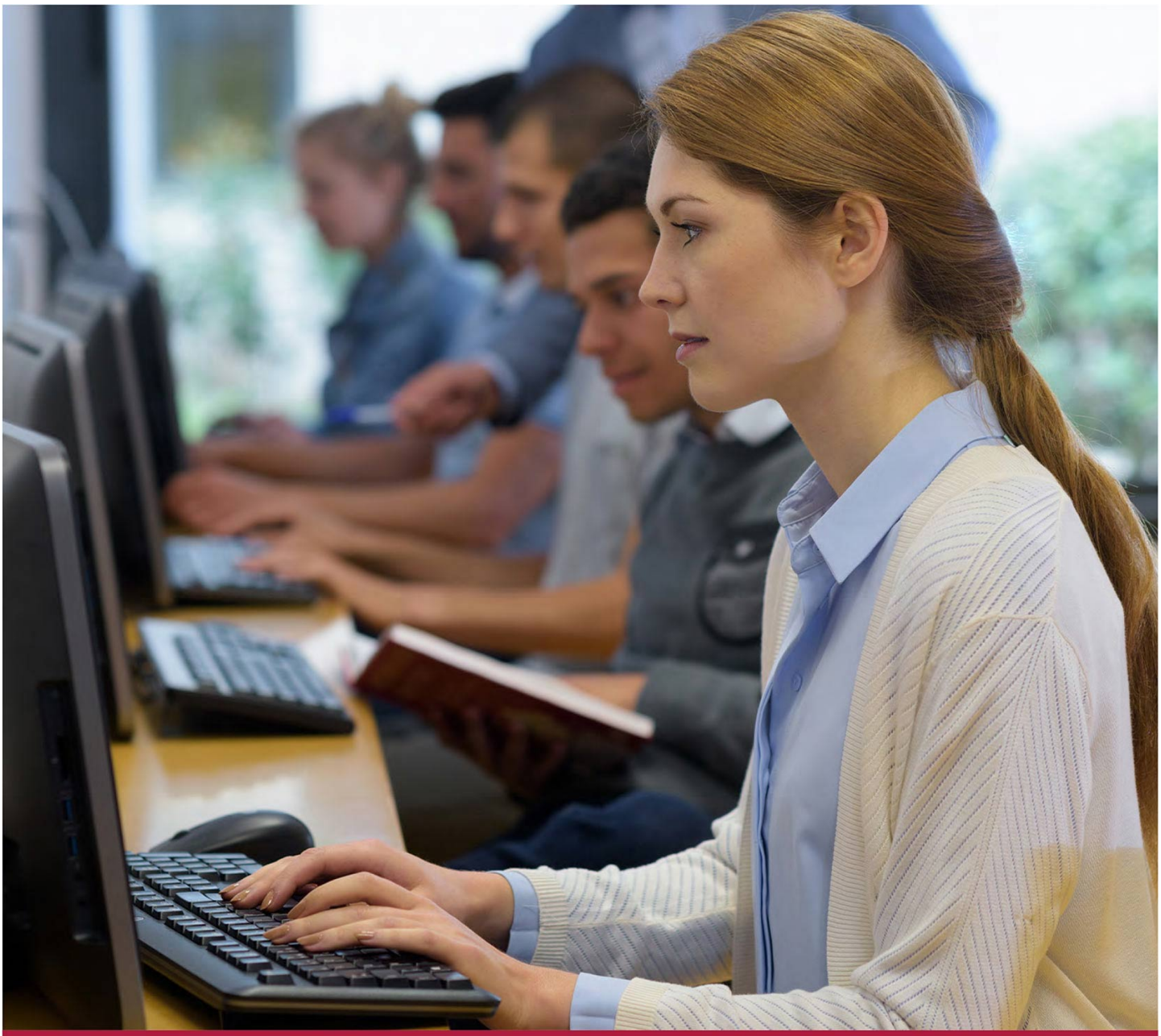
Академия АйТи
a Softline Company



Директор по информационной безопасности

Код курса: CISO

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

© Академия АйТи, 2024

Директор по информационной безопасности

Код курса: CISO

Длительность	256 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В наши дни директор по информационной безопасности должен быть не просто высокоуровневым специалистом в данной отрасли, а, прежде всего, бизнес-лидером, умеющим увидеть пробелы в информационной безопасности компании, предугадать возможные риски и предотвратить возможные проблемы еще до их наступления. Именно поэтому современному CISO (Chief Information Security Officer) необходимо иметь комплексные и системные знания не только о самих цифровых технологиях и программах. Он должен понимать, как выстроить организованную работу возглавляемой им службы информационной безопасности компании, как разработать корпоративные программы и стратегии, обеспечивающие функционирование такой службы, как проводить киберучения, контроль и аудит и как взаимодействовать с центрами реагирования различного уровня. Все это является важной основой для создания условий слаженной работы служб информационной безопасности и ее оперативного реагирования на возникающие проблемы.

Подробная информация

Актуальность:

- Возрастание значимости роли CISO и требований к ней в связи с появлением новых рисков и угроз;
- Сложность трансформации простого специалиста по информационной безопасности в бизнес-лидера;
- Важность профессионального роста как внутри компании, так и в комьюнити специалистов за ее пределами;
- Расширение профессиональной экспертизы с помощью обучения современным методам и инструментам;
- Компетентный CISO = формирование команды из специалистов высокого уровня.

Целевая аудитория:

- Для сотрудников и специалистов служб информационной безопасности, желающих перейти на уровень директора;
- Для директоров по информационной безопасности, имеющих потребность в устранении

© Академия АйТи, 2024

пробелов в своих знаниях и навыках, входящих в функционал руководителя;

- Для директоров смежных направлений, выполняющих в том числе обязанности CISO без официального назначения.

Обучение на программе позволит вам:

- Освоить насыщенную программу, структурировать имеющиеся знания и приобрести новые;
- Совместить в своей профессиональной экспертизе умение работать с нормативными документами, программами и технологиями и более глубокое мышление руководителя;
- Реализовывать на практике Корпоративную программу управления информационной безопасности в технологически развитых государственных и коммерческих организациях;
- Успешно формировать стратегию работы службы информационной безопасности внутри компании и адаптировать ее работу для противодействия актуальным рискам и угрозам;
- Улучшить системный взгляд на обеспечение информационной безопасности организации, используя для этого актуальные современные методы, ставить приоритетные задачи перед своими подчиненными и грамотно их распределять.

Программа курса

Модуль №1. Стратегия.

- Вызовы и угрозы безопасности. Ландшафт угроз безопасности. Информационная безопасность: понятия и определения, основные подходы к управлению информационной безопасностью, основные процессы управления ИБ.
- Обеспечение ИБ в условиях повсеместной цифровизации. Тенденции и перспективы развития. безопасности. Изучение примеров должностных инструкций сотрудника службы ИБ.
- Метрики и меры информационной безопасности. Разработка корпоративных метрик и мер обеспечения ИБ.
- Оценка и построение модели управления ИБ. Разработка Плана первоочередных мероприятий в области ИБ. Ключевые показатели обеспечения ИБ. Соглашения SLA. Система управления информационной безопасностью. Стандартизация систем менеджмента ИБ согласно международным требованиям и рекомендациям (ISO 27000 и ISO 22300). Корпоративная культура и уровни зрелости системы управления информационной безопасностью.
- Основные требования регуляторов в области информационной безопасности: ФСТЭК России. Требования ФСБ России в части криптографической защиты и ГосСОПКА. Требования Банк России и Минцифры в части обеспечения информационной безопасности.
- Организация службы информационной безопасности. Роль и значение Директора службы информационной безопасности. Модель услуг ИБ. Сорсинг услуг ИБ. От центра затрат к бизнес-единице – центру прибыли. Разработка Стратегии информационной безопасности организации.
- Проекты обеспечения информационной безопасности и киберустойчивости. Управление киберрисками.
- Разработка корпоративной методики управления киберрискам. Основные понятия и определения кибербезопасности и устойчивости цифровых экосистем и платформ. Сквозные технологии безопасности Цифровой экономики (AI+Big Data+ETL). Иммунная защита Индустрии 4.0.
- Дополнительно: дискуссионные клубы и консультации с ментором по модулю.

© Академия АйТи, 2024

Модуль №2. Технологии.

- Адаптация Корпоративной программы управления информационными активами. Разработка моделей угроз безопасности и нарушителя. Методики оценивания ущерба (экономического, социального, экологического) от кибератак злоумышленников.
- Контроль и аудит системы управления информационной безопасностью организации. Проектирование корпоративной системы управления ИБ. Внедрение корпоративной системы управления ИБ.
- Реализация многоуровневого подхода к защите современных цифровых платформ. Эталонные архитектуры безопасных цифровых платформ. Обеспечение ИБ на этапе разработки ПО, эксплуатации и сопровождения.
- Сквозные информационные технологии: Доверенная цифровая технология «Нейротехнологии и Искусственный интеллект». Цифровые технологии: «Квантовые технологии», «Новые производственные технологии».
- Технология «Системы распределенного реестра, DLT или блокчейн», цифровая технология «Компоненты робототехники и сенсорика». Разработка и реализация корпоративной программы повышения осведомленности по вопросам ИБ. Организация и проведение киберучений.
- Организация взаимодействия с национальными и региональными центрами реагирования на инциденты ИБ. Возврат инвестиций на ИБ, методики расчета.
- Дополнительно: дискуссионные клубы и консультации с ментором по модулю.

Модуль №3. Лидерство.

- Онлайн коворкинг.
- Культура в компании и управление людьми в процессе изменений.
- Формирование команды, готовой к современным вызовам.
- Креативное мышление. Культура инноваций.
- Управление изменениями и борьба с сопротивлением.
- Эмоциональный интеллект.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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

© Академия АйТи, 2024