Moscow
Business School
Leadership Energy

Информационная безопасность компании

Срок обучения: 1 день

Время проведения: ежедневно с 10:00 до 17:30

Выдаваемые документы: Удостоверение о повышении квалификации или Сертификат Moscow Business School

Программа обучения

Информационная безопасность. ИТ-безопасность. Кибербезопасность. Технические средства защиты информации

- Тренды информационной безопасности в России и мире: что нужно знать бизнесу?
- Политики информационной безопасности. Менеджмент информационной безопасности. Стандарты информационной безопасности. Аудит информационной безопасности организации. Влияние политик информационной безопасности на кибербезопасность организации. Аудит эффективности отделов ИТ и ИБ
- Риски информационной безопасности в условиях виртуального мира, удаленного подключения и облачного присутствия. Страхование кибер рисков и рисков информационной безопасности
- Технологии искусственного интеллекта и машинного обучения — решения для кибербезопасности. Угрозы и уязвимости организации, связанные с внедрением в практику систем искусственного интеллекта. Нейросети для систем мониторинга событий информационной безопасности и совершенствования средств защиты информации
- Актуальные вопросы информационной безопасности беспилотных летательных аппаратов и другого беспилотного транспорта. Проблемы противодействия БПЛА на каналах связи и управления
- Ландшафт современных киберугроз и подходы к автоматическому реагированию. Актуальные вопросы противодействия кибертерроризму. Практика противодействия кибератакам и построения центров мониторинга

информационной безопасности. Автоматизация реагирования на инциденты информационной безопасности. Основные виды атак на инфраструктуру. Кража данных с помощью программ-вымогателей

- первоочередные меры по повышению защищенности ИТ-инфраструктуры. Обзор изменений законодательства в области информационной и кибербезопасности за 2022 — 2023 гг. Вопросы разграничения ответственности за защиту информации при удаленном взаимодействии
- Вопросы построения защиты объектов критической информационной инфраструктуры (КИИ). Защита объектов КИИ: актуальные проблемы и прогноз. Киберразведка на объектах КИИ. Импортозамещение критических объектов. Влияние импортозамещения в информационной безопасности на защиту объектов КИИ. Проблемы импортозамещения компонентов объектов КИИ. Импортозамещение систем защиты от утечек информации. Актуальные вопросы моделирования угроз безопасности объектов КИИ
- Актуальные вопросы построения системы защиты автоматической системы управления технологическим процессом (АСУ ТП). Повышение защищенности АСУ ТП. Безопасный удаленный доступ и защита АСУ ТП. Подходы к организации дистанционного доступа к корпоративным информационным системам. Кибербезопасность объектов топливно-энергетического комплекса
- Основные требования, предъявляемые к персоналу информационных систем, при приеме на работу, во время работы и при увольнении в части соблюдения правил информационной безопасности. Особенность работы с работниками, работающими в удаленном режиме. Аутсорсинг информационной безопасности. Подходы к подготовке персонала цифровых предприятий в условиях перехода на технологический суверенитет
- Технические и организационные средства защиты информации. Обзор решений класса DLP. Информационная безопасность облаков: основные тенденции и новые решения

Практикум «Разбор кейсов по последним требованиям технической и информационной безопасности»