INTERNATIONAL BUSINESS ACADEMY

+7 727 328 02 02/03 hotline 24/7

+7 702 777 44 11

Информационная безопасность организации

Программа

Блок 1. Защита информации как составная часть общей системы безопасности организации

- Понятие информационной безопасности. Наиболее распространенные угрозы. Основные определения и критерии классификации угроз.
- Основные направления защиты информации.
- Понятие системы менеджмента информационной безопасности. Недостатки проектного подхода к построению системы управления информационной безопасностью. Процессный подход к обеспечению информационной безопасности.
- Международные стандарты безопасности информационных систем. Стандарт, базирующиеся на процессном подходе к обеспечению информационной безопасности — ISO 27001. ISO 27001 и национальные нормативные документы по ИБ. Требования ISO 27001.
- Политика информационной безопасности как основа системы менеджмента ИБ. Цели и задачи Политики информационной безопасности. Общая структура Политики информационной безопасности.
- Аудит состояния информационной безопасности на предприятии. Порядок проведения аудита информационной безопасности в организации.
- Программные средства, поддерживающие управление информационной безопасностью на предприятии.

Блок 2. Противодействие промышленному шпионажу. Техническая защита информации

- Классификация технических каналов утечки информации.
- Технические каналы утечки акустической информации.
- Защита акустической (речевой) информации.
- Средства и методы обнаружения технических каналов утечки информации.
- Мероприятия по выявлению технических каналов утечки информации. Оценка защищенности информации от утечки по ТКУИ.

Блок 3. Режим коммерческой тайны. Конфиденциальное делопроизводство

- Коммерческая тайна. Понятие «коммерческой тайны» в предпринимательской деятельности. Нормативно-правовые акты РК, определяющие понятие коммерческая тайна.
- Порядок создания режима коммерческой тайны в организации.
- Составление и применение перечня сведений, составляющих коммерческую тайну организации, рекомендуемая информация, которая должна составлять коммерческую тайну организации.
- Процедура ограничения доступа к информации, составляющей коммерческую тайну организации.
- Внутренние нормативные документы, регламентирующие деятельность организации в области защиты коммерческой тайны. Изменения и дополнения, вносимые в нормативно-правовые документы организации при введении режима коммерческой тайны.
- Обязательство работника по сохранению коммерческой тайны организации.
- Соблюдение режима коммерческой тайны в договорной работе.
- Процедура передачи государственным органам информации, составляющей коммерческую тайну организации.
- Виды юридической ответственности за разглашение коммерческой тайны, а также за незаконное получение информации.
- Конфиденциальное делопроизводство — составная часть системы безопасности организации. Конфиденциальное делопроизводство как элемент режима защиты коммерческой тайны.
- Принципы построения конфиденциального делопроизводства.
- Порядок взаимодействия открытого и конфиденциального делопроизводства.
- Этапы создания конфиденциального делопроизводства, практические

рекомендации по порядку создания.

Блок 4. Методы и средства защиты компьютерных систем (IT-безопасность, кибербезопасность). Подразделение информационной безопасности

- Возможность защиты информации при работе в сети Internet. Межсетевое экранирование.
- VPN (виртуальная частная сеть). Преимущества организации виртуальных частных сетей на основе Internet.
- Активный аудит.
- Основы криптографической защиты информации. Классификация методов криптографического закрытия информации.
- Электронная цифровая подпись как базовый механизм обеспечения юридической силы документа при электронном документообороте и наиболее эффективное средство подтверждения авторства и подлинности электронного документа.
- Практические примеры применения криптографических методов защиты информации.
- Подразделение информационной безопасности. Какой быть структуре эффективного подразделения информационной безопасности? Место подразделения ИБ в структуре организации. Разделение функций между подразделением ИБ и IT-подразделением.
- Организация взаимодействия с руководством подразделения информационной

безопасности и руководителями структурных IT-подразделений организации.

Блок 5. Минимизация ущерба от угроз утечки и разглашения информации со стороны «человеческого фактора»

- Угрозы организации со стороны сотрудников.
- Мотивированное и немотивированное разглашение информации.
- Психологические особенности сотрудников, представляющих опасность для организации. Схема проверки кандидатов (соискателей) на работу.
- Превентивные мероприятия, проводимые Службой безопасности организации по предотвращению утечки информации со стороны сотрудников организации.
- Различные варианты создания стимулов и мотивационных факторов, направленных на усиление лояльности сотрудников организации.
- Создание системы персональной ответственности сотрудников организации.
- Порядок проведения внутрикорпоративных проверок (расследований) по фактам утечки и разглашения информации со стороны сотрудников организации.
- «Растровые признаки опасности» у сотрудников. На что обратить внимание в проверочных мероприятиях.

Блок 6. Актуальные вопросы защиты персональных данных

- Закон «О персональных данных», основные нормы закона, применяемые термины и определения. Трудовой кодекс РК и иные нормативно-правовые акты РК, регламентирующие вопросы персональных данных и их защиту. Международные конвенции по защите персональных данных физических лиц.
- Общие вопросы обработки и обеспечения защиты персональных данных (ПДн) в компании.
- Общие вопросы проведения работ по комплексной защите ПДн.
- Порядок проведения проверок регуляторами в области защиты персональных данных.
- Обзор основных мероприятий, нормативно-правовой, организационно-распорядительной и нормативно-технической документации при создании системы защиты ПДн.
- Виды ответственности за разглашение персональных данных, а также за ее незаконное получение. Необходимые и достаточные условия для ее наступления.

По окончании участники смогут:

- Организовать систему защиты информации на предприятии
- Эффективно противодействовать промышленному шпионажу
- Организовать работу по защите персональных данных
- Минимизировать ущерб от угроз утечки и разглашения информации со стороны «человеческого фактора»

INTERNATIONAL BUSINESS ACADEMY

+7 727 328 02 02/03 hotline 24/7

+7 702 777 44 11

РК, г. Алматы ул. Шашкина 24БЦ K Plaza офис 1 (уг. проспекта Аль-Фараби)

www.iba.kz

info@iba.kz