

**СЕМИНАР-ПРАКТИКУМ:**

**«ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РУКОВОДИТЕЛЕМ СБ.**

**ОБЕСПЕЧЕНИЕ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ И ПЕРСОНАЛЬНЫХ ДАННЫХ»**

(2 дня – 16 акад. часов)

|  |
| --- |
| **Первичная целевая аудитория:** |
| 1. Собственники и руководители Компаний. 2. Руководители по безопасности. 3. Руководители служб внутреннего контроля. 4. Руководители юридического подразделения. 5. Руководители подразделений информационной безопасности. 6. Руководители ИТ-подразделений. |
| **Вторичная целевая аудитория:** |
| 1. Сотрудники безопасности. 2. Сотрудники ИТ - подразделений. 3. Специалисты по внутреннему контролю. 4. Сотрудники кадровых подразделений. 5. Сотрудники служб маркетинга и рекламы. |
| **Что в результате получит слушатель:** |
| * Систематизированные знания по организации информационной безопасности. * Навыки по взаимодействию подразделений ИТ с сотрудниками служб безопасности в целях защиты информации. * Рекомендации по определению и введению режима коммерческой тайны на предприятии. * Рекомендации по организации информационно-аналитического обеспечения безопасности в направлении защиты информации. * Навыки по противодействию утечке коммерческой тайны, конфиденциальной информации и персональных данных. * Обоснование организационной структуры, прав, ответственности и полномочий сотрудников ИТ - подразделений и информационной безопасности. * Рекомендации по организационному, методическому и нормативному обеспечению подразделений отвечающих за контроль и противодействие экономическому шпионажу**.** |

**1 ДЕНЬ**

**«Организация системы информационной безопасности руководителем СБ»**

* законодательство Российской Федерации в области защиты информации. Международные стандарты безопасности информационных систем. Американская концепция системного подхода к обеспечению защиты конфиденциальной информации (OPSEC Operation Security);
  + нормативные акты, положения, политики и инструкции в области защиты информации в России и в мире (законы, подзаконные акты, ГОСТы, РД, ISO и т.п.)
* основные вопросы при организации ИБ на предприятии. Организационное и техническое обеспечение информационной безопасности (ИБ) в компании. Деление информации по уровням конфиденциальности;
* правовые, организационные, режимные и инженерно-технические мероприятия по защите конфиденциальной информации. Создание внутриобъектового и контрольно-пропускного режимов на предприятии. Физическая защита охраняемых информационных ресурсов;
* Анализ рисков. Принципы снижения рисков ИБ. Методика разработки Политики информационной безопасности предприятия. Общая схема безопасности корпоративной информационной системы;
* Подготовка необходимых документов для Службы Безопасности. Модель угроз. Модель действия нарушителя и т.п. Элементы защиты и технологии защиты информации;
* Контроль использования ресурсов сети Интернет сотрудниками компании. Проблематика обеспечения безопасности при использовании беспроводных технологий Wi-Fi. Практическое построение защищенной сети;
* Применение средств инструментального контроля для анализа обеспечения безопасности (внешний, внутренний аудит).

***ТЕСТ: «Информационная безопасность и защита информации»***

***ЗАДАНИЕ: «Анализ рисков ИБ в Компании»***

**2 ДЕНЬ**

**«Обеспечение безопасности коммерческой тайны в организации. Методики и практические аспекты»**

* законодательство РФ о коммерческой тайне. Понятие режима коммерческой тайны;
* коммерческая тайна в системе обеспечения безопасности деятельности предприятия. Ее место и роль;
* формирование в Компании перечня сведений, составляющих коммерческую тайну. Создание конфиденциального делопроизводства;
* правовые, режимные, технические и ИТ мероприятия по защите коммерческой тайны. Виды юридической ответственности за разглашение коммерческой тайны, а также за незаконное получение этой информации. Необходимые и достаточные условия для ее наступления;
* разработка корпоративной правовой базы для функционирования режима коммерческой тайны;
* законодательство РФ о защите персональных данных. Основные требования федерального закона «О персональных данных» и правовых актов регуляторов в части защиты персональных данных. Государственный контроль за обработкой в компаниях персональных данных;
* организационные, правовые и технические требования по обработке персональных данных. Алгоритмы и пошаговые действия предприятия по выполнению требований законодательства в области обработки персональных данных;
* особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Подготовка организационно-распорядительной документации на предприятии по защите персональных данных;
* расследование случаев, связанных с разглашением информации, составляющей коммерческую тайну или персональные данные, похищением или утерей документов;
* Психологические приемы общения с проверяющими и контролирующими органами. Правовые аспекты сохранения коммерческой тайны и персональных данных при работе с проверяющими органами.
* Техническая защита сведений, составляющих коммерческую тайну и персональные данные.

***ТЕСТ: «Коммерческая тайна и персональные данные»***

***ЗАДАНИЕ: «Отнесение информации к коммерческой тайне»***