



Пособие адресовано руководителям и специалистам предприятия, отвечающим за защиту информации. Оно может также стать интересным и полезным для студентов (слушателей), изучающих курс по защите информации и готовящихся к серьезной и эффективной практической работе по противодействию экономическому шпионажу на предприятии. Как показывает многолетний опыт подготовки и переподготовки таких специалистов во многих учебных заведениях, в настоящее время имеется острый дефицит кадров, обладающих основательными практическими знаниями в этой области.

Введение

Глава 1. Из истории экономического шпионажа

- 1.1. Экономический шпионаж в современном обществе
- 1.2. Отечественный промышленный шпионаж

Глава 2. Экономический шпионаж – важнейшая угроза безопасности предприятию

- 2.1. Экономический шпионаж и ваш бизнес
- 2.2. Экономический шпионаж как важнейшая угроза безопасности бизнеса
- 2.3. Система противодействия экономическому шпионажу
- 2.4. Инсайдер – главный нарушитель информационной безопасности

Глава 3. Наемный персонал предприятия – основная причина и источник экономического шпионажа на предприятии

3.1. Правовые аспекты мероприятий по противодействию экономическому шпионажу на предприятии

- 3.1.1. Режим коммерческой тайны как способ противодействия экономическому шпионажу
- 3.1.2. Правовые аспекты и критерии установления режима коммерческой тайны
 - 3.1.2.1. Правовые основы построения системы обеспечения безопасности информации
 - 3.1.2.2. Права обладателя информации, составляющей коммерческую тайну
 - 3.1.2.3. Меры по охране конфиденциальности информации
 - 3.1.2.4. Охрана конфиденциальности информации в рамках трудовых отношений
 - 3.1.2.5. Охрана конфиденциальности информации в рамках гражданско-правовых отношений
 - 3.1.2.6. Охрана конфиденциальности информации при ее предоставлении
 - 3.1.2.7. Ответственность за нарушение требований Федерального закона «О коммерческой тайне»
- 3.1.3. Порядок отнесения сведений к коммерческой тайне
 - 3.1.3.1. Правовые основы отнесения информации к информации, составляющей коммерческую тайну, и способы получения такой информации
 - 3.1.3.2. Порядок разработки перечня сведений конфиденциального характера
 - 3.1.3.3. Определение и установка грифа (пометки), снятие (изменение) грифа (пометки) конфиденциальности, содержащихся в работах, документах и изделиях
- 3.1.4. Перечень лиц, допущенных к сведениям отнесенных к коммерческой тайне
 - 3.1.4.1. Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных
 - 3.1.4.2. Допуск должностных лиц, работников к конфиденциальной информации
 - 3.1.4.3. Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных
 - 3.1.4.4. Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну
 - 3.1.4.5. Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям

3.2. Организационные мероприятия по противодействию экономическому шпионажу

- 3.2.1. Изучение персонала при приеме и расстановке кадров
 - 3.2.1.1. Особенности приема лиц и перевода работников на работу, связанную с владением конфиденциальной информацией
 - 3.2.1.2. Текущая работа с персоналом, владеющим конфиденциальной информацией
 - 3.2.1.3. Особенности увольнения работников, владеющих конфиденциальной информацией

- 3.2.2. Методы и способы выявления лиц, способных нанести финансовый материальный ущерб предприятию
 - 3.2.2.1. Методы получения ценной информации у работников
 - 3.2.2.2. Типовые формы и методы реализации угроз информационной безопасности организации с участием персонала
 - 3.2.2.3. Методы противодействия угрозам информационной безопасности организации со стороны персонала
- 3.2.3. Конфиденциальное делопроизводство как способ противодействия экономическому шпионажу
 - 3.2.3.1. Основы организации и ведение специального делопроизводства
 - 3.2.3.2. Организация службы делопроизводства
 - 3.2.3.3. Структуры службы делопроизводства
 - 3.2.3.4. Система учета документированной информации, носителей информации
 - 3.2.3.5. Разработка и оформление конфиденциальных документов на рабочих местах
 - 3.2.3.6. Уничтожение документов, дел и других носителей конфиденциальной информации
 - 3.2.3.7. Подготовка к эвакуации и эвакуация носителей сведений, составляющих конфиденциальную информацию. Работа с ними в чрезвычайных ситуациях
 - 3.2.3.8. Порядок передачи дел и должности при смене должности, увольнении
- 3.2.4. Режим безопасности при создании конфиденциальных изделий и обращение с ними
 - 3.2.4.1. Режим безопасности при создании конфиденциальных изделий
 - 3.2.4.2. Порядок учета конфиденциальных изделий
 - 3.2.4.3. Хранение и передача конфиденциальных изделий
 - 3.2.4.4. Учет, хранение конфиденциальной технической документации и обращение с ней

3.3. Технические средства контроля персонала на предприятии

- 3.3.1. Технические средства наблюдения
 - 3.3.1.1. Системы телевизионного наблюдения
 - 3.3.1.2. Особенности телевизионного наблюдения
- 3.3.2. Контроль телефонных переговоров
 - 3.3.2.1. Аппаратура для мониторинга телефонных линий
- 3.3.3. Технический контроль информационных систем
 - 3.3.3.1. Применение кейлоггеров для контроля за персоналом
 - 3.3.3.2. Мониторинг электронной почты

Глава 4. Характеристика источников угроз безопасности, технических каналов утечки информации (ТКУИ) и мероприятий по защите информации

- 4.1. Угрозы безопасности информации, реализуемые техническими средствами промышленного шпионажа**
- 4.2. Использование особенностей технических средств с учетом факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях**
 - 4.2.1. Использование особенностей технических средств, установленных в выделенных помещениях (ВП)
 - 4.2.2. Особенности выявления и перехвата побочных электромагнитных излучений (ПЭМИ) и наводок (ПЭМИН)
 - 4.2.3. Информационная безопасность беспроводных средств связи (БСС)
 - 4.2.4. Использование технических средств, имеющих в своем составе программируемые элементы
 - 4.2.5. Информационная безопасность технических средств, входящих в состав сетей различного назначения
 - 4.2.6. Информационная опасность подключения к сети Интернет
 - 4.2.7. Радиоизлучения (электрические сигналы) от внедренных специальных электронных устройств перехвата информации (СЭУ ПИ в том числе закладочных устройств)
- 4.3. Каналы утечки информации и преднамеренного и несанкционированного воздействия на информацию**
 - 4.3.1. Технический канал утечки информации
 - 4.3.2. Каналы несанкционированного воздействия (НСВ)
 - 4.3.3. Каналы силового деструктивного воздействия (СДВ) и преднамеренного воздействия (ПДВ)
- 4.4. Организация проведения специальных исследований (СИ)**
 - 4.4.1. Перечень мероприятий, которые необходимо проводить при специальных исследованиях
 - 4.4.2. Порядок организации и проведения специальных исследований технических средств обработки информации

- 4.4.3. Специальные исследования в области защиты речевой (акустической) информации
 - 4.4.4. Специальные исследования в области акустоэлектрических преобразований (АЭП)
 - 4.4.4.1. Эквивалентная схема акустоэлектрического преобразовательного элемента
 - 4.4.4.2. Схемы электроакустических преобразователей
 - 4.4.4.3. Средства и системы, подлежащие обязательному анализу на объектах специальных исследований на предмет АЭП
 - 4.4.4.4. Схемы и средства измерения
 - 4.4.5. Специальные исследования побочных электромагнитных излучений и наводок
 - 4.4.5.1. Теоретические основы
 - 4.4.5.2. ПЭВМ как источник электромагнитных излучений
 - 4.4.5.3. Простые измерительно-расчетные способы определения информативных ПЭМИ
 - 4.4.6. Структура и содержание документов по специальному исследованию основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС). Порядок подготовки документов
 - 4.4.7. Предписание на эксплуатацию
 - 4.4.8. Оформление результатов специальных исследований
 - 4.4.9. Порядок проведения специальных исследований ОТСС и ВТСС
- 4.5. Специальные проверки (СП) и специальные обследования (СО)**
- 4.5.1. Специальные устройства перехвата информации
- 4.6. Специальное обследование помещений**
- 4.6.1. Порядок выполнения поисковых мероприятий
 - 4.6.2. Отчетные материалы по СО выделенных помещений (ВП)
- 4.7. Специальная проверка технических средств**
- 4.7.1. Порядок проведения специальной проверки технических средств
 - 4.7.2. Обнаружение металлических предметов с использованием металлодетектора
 - 4.7.3. Приборы рентгеновизуального контроля
 - 4.7.4. Тепловизионные приборы
 - 4.7.5. Технические эндоскопы
 - 4.7.6. Средства радиационного контроля

Глава 5. Организационно-технические мероприятия и технические способы защиты информации защищаемого помещения

- 5.1. Организация защиты информации
- 5.2. Порядок и состав проводимых работ по защите информации на объекте информатизации
- 5.3. Организационно-технические мероприятия
- 5.4. Защита информации техническими способами и средствами
- 5.5. Особенности комплексной защиты информации
- 5.6. Основные требования и рекомендации по защите информации, циркулирующей в технических средствах и защищаемых помещениях
- 5.7. Способы и средства подавления электронных устройств перехвата информации
- 5.8. Комплексная защита телефонных линий связи
 - 5.8.1. Возможные «угрозы» абоненту телефонной линии связи
 - 5.8.2. Средства защиты информации передаваемой по телефонным линиям связи
 - 5.8.3. Способы защиты телефонных линий

Глава 6. Аттестация объектов информатизации

- 6.1. Общие положения
- 6.2. Порядок проведения аттестации объектов информатизации
- 6.3. Аттестационные испытания

Приложение

- Приложение 1.
- Приложение 2.
- Приложение 3.
- Приложение 4.

Список литературы