Противодействие экономическому шпионажу на предприятии

105 стр. PDF 2020 г.

Пособие адресовано руководителям и сотрудникам предприятий и организаций, отвечающим за защиту информации на вверенном объекте. 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 в государственных и коммерческих структурах. Как показывает многолетний опыт подготовки и переподготовки таких специалистов в учебном центре «Маском», в РГГУ, в Финансовой Академии при Правительстве РФ и других учебных заведениях, в настоящее время наблюдается острый дефицит специалистов, обладающих основательными практическими знаниями в этой области.

Пособие состоит из 9 разделов, где рассмотрены правовые, организационные и технические аспекты противодействия экономическому шпионажу, приведены данные исследований и статистики по работе с конфиденциальными документами и изделиями, по грамотной работе с персоналом, по организационным мероприятиям в области защиты информации, описываются источники угроз информационной безопасности, технические каналы утечки информации.

Ценность пособия заключается в том, что в нем рассмотрен практически весь комплекс вопросов, имеющих прямое отношение к противодействию экономическому шпионажу. При этом учтены как современные наработки в борьбе с инсайдерством, так и основополагающие требования по защите технических каналов утечки информации.

Введение

Глава 1. Из истории экономического шпионажа

1.1. Основные понятия и исторические этапы становления экономического шпионажа

1.2. Экономический шпионаж в современном обществе

1.3. 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

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

3.1. Инсайдер – главный нарушитель информационной безопасности

3.2. Классификация нарушителя

Категории нарушителя

Разработка модели нарушителя

Основные мотивы нарушений

3.3. Методы и способы несанкционированного доступа нарушителя к защищаемой информации

Каналы утечки информации

Способы и методы добывания информации

3.4. Методы получения ценной информации у работников

3.5. Типовые формы и методы реализации угроз ИБ организации с участием персонала

Систематизированный перечень методов и способов реализации угроз информационной безопасности в организации

Наиболее распространенные формы нарушения персоналом требований режима защиты информации

Контроль за сотрудниками организации

3.6. **Методы противодействия угрозам ИБ организации со стороны персонала**

Формирование ранжированного перечня конфиденциальных сведений организации как объекта защиты

Оценка возможных каналов утечки (перехвата) конфиденциальной информации организации

Определение перечня прикладных методов защиты информации

Внедрение системы обеспечения ИБ организации

Глава 4. Правовые аспекты мероприятий по противодействию экономическому шпионажу на предприятии

4.1. **Правовые основы построения системы обеспечения безопасности информации**

4.2. **Права обладателя информации, составляющей коммерческую тайну**

4.3. **Правовые основы отнесение информации к сведениям, составляющим коммерческую тайну**

4.4. **Меры по охране конфиденциальности информации**

4.5. **Охрана конфиденциальности информации в рамках трудовых отношений**

Обязанности работодателя в целях охраны конфиденциальности информации

Обязанности работника в целях охраны конфиденциальности информации

4.6. **Охрана конфиденциальности информации в рамках гражданско-правовых отношений и при ее предоставлении органам государственной власти**

4.7. **Ответственность за нарушение требований Федерального закона «О коммерческой тайне»**

Глава 5. Режимные мероприятия по противодействию экономическому шпионажу

5.1. **Режим коммерческой тайны – как способ противодействия экономическому шпионажу**

Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации

Условия для реализации угроз при работе с конфиденциальной информацией

Направления работ для обеспечения режима конфиденциальности

5.2. **Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных**

Принципы построения разрешительной системы доступа

Задачи разрешительной системы

5.3. **Допуск должностных лиц, работников к конфиденциальной информации**

5.4. **Доступ должностных лиц, работников к конфиденциальным информации, документам и БД**

5.5. **Обязанности должностных лиц, допущенных к сведениям, составляющим конфиденциальную информацию**

Обязанности работников, допущенных к сведениям, составляющим КИ

Запреты для работников, допущенных к сведениям конфиденциального характера

5.6. **Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям**

Глава 6. Работа с персоналом как основной способ противодействия экономическому шпионажу

6.1. **Особенности приема лиц и перевода работников на работу, связанную с владением конфиденциальной информацией**

Подготовительные этапы процесса приема лиц на работу

Направления активного поиска кандидатов на вакантную должность

Проверка документов, предоставленных кандидатом

Психологический отбор

6.2. **Текущая работа с персоналом, владеющим конфиденциальной информацией**

Обучение работников предприятия правилам защиты информации

Общие методические требования к организации подготовки работника

Здоровый психологический климат в коллективе

Превентивный контроль работы сотрудников

Аттестация работников

6.3. **Особенности увольнения работников, владеющих конфиденциальной информацией**

Глава 7. Конфиденциальное делопроизводство – как способ противодействия экономическому шпионажу

7.1. Основы организации и ведение специального делопроизводства

7.2. Организация службы делопроизводства

Централизованная форма

Децентрализованная форма

Смешанная форма

7.3. Система учета носителей информации и регистрации документированной информации

7.4. Разработка и оформление конфиденциальных документов

7.5. Уничтожение документов, дел и других носителей конфиденциальной информации

7.6. Подготовка к эвакуации и эвакуация носителей конфиденциальных сведений, работа с ними в чрезвычайных ситуациях

Глава 8. Контроль персонала по выполнению ими требований режима конфиденциальности

8.1. Основные положения по осуществлению контроля

Причины проверки выполнения требований нормативных документов

Основные принципы контроля обеспечения режима безопасности и защиты информации

Задачи при проверке режима безопасности и защиты информации в подразделении

8.2. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа

8.3. Проведение служебного расследования по фактам нарушения требований режима безопасности

8.4. Проверка носителей сведений ограниченного доступа при смене начальников подразделений

Глава 9. Технические средства контроля персонала на предприятии

9.1. Технические средства для наблюдения за персоналом

9.2. Системы телевизионного наблюдения

9.3. Особенности телевизионного наблюдения

9.4. Контроль телефонных переговоров

Автоматический мониторинг телефонных линий с помощью аппаратуры «Спрут»

Многоканальная система регистрации VOCORD Phobos Audio

Модуль системы VOCORD Phobos для декодирования факсимильных сообщений VOCORD SuperFax

Программный модуль системы для определения маршрутов звонков внутренних абонентских линий VOCORD CDR/SMDR

9.5. Технический контроль информационных систем

Анализ клавиатурного почерка

Кейлоггеры

9.6. DLP-системы

Назначение DLP-системы

Цели внедрения DLP-системы

Задачи, решаемые при внедрении DLP-системы

Что хранить в архиве

Как DLP облегчает расследование

Литература