Аналитическая работа в службе защиты информации

Тема. 3
Основные этапы аналитической работы

В аналитической работе можно выделить следующие основные этапы:

1. формулирование целей аналитической работы, разработка программы исследований, формулирование предварительных гипотез (результатов аналитической работы);
2. отбор и анализ источников информации, сбор и обобщение информации;
3. полноценный анализ имеющейся информации и подготовка выводов.

Типовая программа исследований включает следующие основные разделы:

1. цели и задачи аналитического исследования;
2. предметы и объекты исследования;
3. сроки (период) проведения аналитического исследования;
4. методики проведения исследования;
5. ожидаемые результаты и предполагаемые выводы.

Наиболее типичны следующие задачи аналитического исследования:

1. получение данных о состоянии системы защиты информации на предприятии (его конкретных объектах, в филиалах, представительствах);
2. выявление возможных каналов утечки информации, подлежащей защите;
3. определение обстоятельств, причин и факторов, способствующих возникновению каналов утечки и созданию предпосылок для утечки информации;
4. подготовка для руководства предприятия (филиала, представительства) и его структурных подразделений конкретных рекомендаций по закрытию выявленных каналов утечки.

Под объектом исследования понимается все то, что изучается и анализируется в ходе исследования.

Предмет исследования — та сторона объекта, которая непосредственно подлежит изучению в ходе аналитического исследования.

Особое значение на первом этапе аналитической работы имеет формулирование предварительных гипотез (версий).

Предварительные гипотезы должны объяснить роль и место выводов аналитических исследований в логической последовательности происходящих событий в сфере защиты охраняемой информации.

Построение предварительных гипотез проводится в следующем порядке.

1. Формируется полный список сведений, которые предполагается исследовать (проанализировать). Вошедшие в список сведения систематизируются и располагаются по степени важности.

2. Из всего объема информации выделяется группа наиболее значимых сведений, роль которых особенно очевидна в ситуации, подлежащей анализу и оценке. Выбранные сведения классифицируются по актуальности, способу получения и степени достоверности источника. Наиболее актуальные сведения анализируются в первую очередь.

3. Проводится выбор предварительных гипотез, объясняющих проявления тех или иных событий (появление тех или иных сведений). Причем в отношении одного события осуществляется проверка нескольких гипотез (версий). При последовательной проверке гипотез особое внимание уделяется наиболее реальным. Эти гипотезы фиксируются. Наименее реальные гипотезы отклоняются.

Таким образом, последовательно выбираются и формулируются наиболее вероятные предположения, объясняющие появление тех или иных конкретных событий (возникновение сведений). Возможные противоречия в полученных выводах о предполагаемых версиях происходящих событий устраняются путем всесторонней последовательной проверки реальности гипотез.

Результатом работы по формулированию предварительных гипотез является выбор версии, которая наиболее точно, по сравнению с другими версиями, объясняет причину возникновения конкретной ситуации, связанной с появлением возможного канала утечки конфиденциальной информации, и характеризует состояние системы защиты информации, в том числе — действия соответствующих должностных лиц, качество выполнения мероприятий и т.д.

На втором этапе проводится отбор и анализ источников информации, сбор и обобщение данных в целях выявления канала несанкционированного доступа к сведениям конфиденциального характера, исключения возможности возникновения такого канала.

Дальнейшие этапы…….

Темы ….для практических занятий…..