К ВОПРОСУ О МЕТОДИКЕ ПРЕПОДАВАНИЯ ТЕМЫ «ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ»

А.И. Серый

Учебные планы некоторых физико-математических специальностей (в частности, «Компьютерная физика») предусматривают, среди прочих дисциплин, изучение дисциплины «Технические средства и методы защиты информации» [1]. Важное место в этой дисциплине занимают вопросы, связанные с техническими каналами утечки информации и мерами по борьбе с утечкой информации по таким каналам. Несмотря на бурное развитие указанной дисциплины и довольно быструю потерю актуальности сведений о некоторых конкретных технических устройствах, общие принципы формирования каналов утечки информации и выбора мер борьбы с ними можно считать относительно устойчивыми.

Каждый отдельно взятый технический канал утечки информации можно охарактеризовать по следующим пунктам. 1.1. Тип сигнала (акустический, электрический, электромагнитный). 1.2. Для каждого типа сигнала – подкласс канала (например, акустические каналы бывают воздушными, вибрационными и другими). 1.3. Разновидность устройства съема информации и ее дальнейшей передачи. 2.1. Меры по недопущению проникновения информации в канал утечки (иными словами – меры по устранению или уменьшению демаскирующих признаков (ДП) охраняемого объекта), связанные: а) с понижением уровня исходного сигнала (в том числе путем изоляции); б) с зашумлением сигнала. 2.2. Меры по поиску устройств съема информации: а) по внешним ДП (даже если устройство закамуфлировано); б) по наличию полупроводниковых соединений (с помощью нелинейных локаторов); в) по электромагнитному излучению во время работы (с помощью, технических средств радиомониторинга и других устройств). 2.3. Меры противодействия работе устройств съема информации после обнаружения таких устройств: а) отключение; б) блокировка канала дальнейшей передачи информации; в) вывод устройства из строя. Таким образом, требуется ослабить ДП своих устройств и усилить ДП устройств противника (чьи задачи сформулированы почти или точно так же, но противоположны с точки зрения перечня устройств)

Приоритеты при выборе конкретных мер из перечисленных выше, как правило, обусловлены: а) принципиальными физико-техническими возможностями; б) допустимостью с точки зрения действующего законодательства; в) стремлением к минимуму финансовых издержек. Руководствуясь данным алгоритмом, можно составлять план по реализации мер противодействия утечке информации в конкретных ситуациях. Составление подобных планов можно предлагать учащимся в качестве самостоятельных творческих заданий. Данная публикация является дополнением к [2].

Литература

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Голубятников И.В., Солдатов А.А., Скрыль С.В. Технические средства и методы защиты информации. М.: Горячая линия–Телеком, 2012. 616 с.

2. Серый, А.И. К вопросу о методике преподавания дисциплины технические средства и методы защиты информации» Тезисы докладов XIX Белорусско-российской научно-технической конференции «Технические средства защиты информации», Минск, 8 июня 2021 г. С. 86–87.