Предисловие

Современный этап развития российского общества характеризуется существенным возрастанием понимания роли и актуальности проблем обеспечения безопасности во всех сферах жизнедеятельности. Особенно показателен этот процесс для сферы информационной безопасности, которая за последнее десятилетие вышла из области компетенции сугубо специальных служб и превратилась в мощный сегмент рыночной индустрии современных информационно-телекоммуникационных технологий.

Общепризнанно, что безопасность функционирования сложных организационно-технических систем определяется прежде всего так называемым человеческим фактором, в качестве одной из характеристик которого выступает уровень профессиональной подготовки работников. Как показывают теоретико-методологические исследования проблем информационной безопасности, задача создания системы планомерной подготовки, переподготовки и повышения квалификации кадров играет не менее важную роль наряду с технологическими и техническими аспектами защиты чувствительной (критической) информации. Актуальность такой задачи не подлежит сомнению в связи с возрастающими требованиями к эффективности, надежности и безопасности сложных комплексов, функционирующих на основе использования критических технологий.

Именно поэтому в Доктрине информационной безопасности Российской Федерации развитие системы обучения кадров, используемых в области обеспечения информационной безопасности, отнесено к числу первоочередных мероприятий по реализации государственной политики в рассматриваемой сфере.

Органы государственной власти, а именно Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, как компетентные органы всегда уделяли особое внимание и поддерживали усилия ученых, преподавателей и специалистов по разработке нормативного и методического обеспечения процессов обучения кадров в области технической защиты информации в рамках государственной системы высшего, дополнительного и среднего специального образования. Не секрет, что в настоящее время имеется дефицит в специализированной литературе для подготовки кадров разных образовательных уровней. Это ощущается в различных учебных центрах, занимающихся повышением квалификации специалистов в области технической защиты

информации. Имеющаяся в наличии литература пока не охватывает все аспекты рассматриваемых проблем, а обсуждаемые вопросы часто не имеют достаточной глубины проработки и даже в специализированных пособиях издания 2018 года авторы используют давно устаревший материал.

Особенно остро данный вопрос стоит при решении проблемы выявления закладочных устройств (ЗУ), предназначенных для получения конфиденциальной информации. В нормативно-методических документах о защите персональных данных (ПДн) также определены угрозы безопасности ПДн, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации.

С учетом специфики вопроса необходимо отметить, что в настоящее время данная тема не получила должного освещения в технической литературе. Поэтому, учитывая то, что Федеральным законом ФЗ № 99 от 22 апреля 2011 г. «О лицензировании отдельных видов деятельности» и Постановлением Правительства РФ от 16 апреля 2012 г. № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» разрешено выявлять ЗУ без получения лицензии, обеспечивая собственную информационную безопасность, возникает необходимость в подготовке грамотных специалистов, так как сейчас в коммерческих структурах крайне мало специалистов, которые знают, как правильно это делать.

Кроме того, выявление ЗУ в государственных и коммерческих структурах имеют существенные отличия, связанные, прежде всего, с дисциплиной руководящего состава, касающейся содержания защищаемых помещений.

В предыдущем пособии автора «Защита информации ограниченного доступа от утечки по техническим каналам» [2] подробно была дана характеристика технических каналов утечки информации и рассмотрены вопросы защиты. Однако с момента выпуска пособия прошло уже более четырех лет и многие технические средства морально устарели. Кроме того, активное развитие цифровой радиоэлектроники привело к появлению принципиально новых средств нападения и защиты, а это существенно изменило подходы к проведению комплексных проверок.

В данном специализированном учебном пособии автор, используя данные о последних разработках в области поискового оборудования, существующую литературу и свой опыт работы и методические разработки в данной области, последовательно и в необходимом объеме постарался изложить вопросы, касающиеся организации и осуществления мероприятий по подготовке и проведению работ по выявлению электронных устройств, предназначенных для негласного получения информации в помещениях и технических средствах коммерческой организации для обеспечения в современных условиях её собственной информационной безопасности.