

**Г. А. Бузов**

**Практическое руководство  
ПО ВЫЯВЛЕНИЮ  
специальных  
технических средств  
несанкционированного  
получения информации**

**Москва  
Горячая линия – Телеком  
2010**

УДК 681.3.067  
ББК 32.81  
Б90

**Бузов Г. А.**

**Б90** Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. — М.: Горячая линия — Телеком, 2010. — 240 с: ил.  
**ISBN 978-5-9912-0121-6.**

Последовательно и в необходимом объеме изложены теоретические и практические вопросы и даны методические рекомендации в области организации и осуществления мероприятий по подготовке и проведению работ по выявлению электронных устройств, предназначенных для негласного получения информации. Описаны физические основы возможных технических каналов утечки как речевой информации, так и информации, обрабатываемой техническими средствами. Изложены назначение, основные характеристики и особенности функционирования специальных технических средств. Рассмотрен пакет нормативно-методических документов, регламентирующих деятельность в области защиты информации. Приведены методики принятия решения на защиту от утечки информации конфиденциального характера, а также выполнения специальных проверок при проведении поисковых мероприятий.

Для специалистов, работающих в области защиты информации, руководителей и сотрудников служб безопасности, а также студентов и слушателей курсов повышения квалификации.

**ББК 32.81**

*Адрес издательства в Интернет WWW.TECHBOOK.RU*

Справочное издание

**Бузов Геннадий Алексеевич**

**Практическое руководство по выявлению  
специальных технических средств  
несанкционированного получения информации**

Редактор *Ю. Н. Чернышов*

Художник *В. Г. Ситников*

Компьютерная верстка *Ю. Н. Чернышова*

Подписано в печать 11.03.2010. Формат 60×90 1/16.

Уч. изд. л. 15. Тираж 500 экз. Изд. № 10121.

ISBN 978-5-9912-0121-6

© Г. А. Бузов, 2010

© НТИ «Горячая линия—Телеком», 2010

# 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.

При мощном прогрессе области технической защиты информации 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.

Проблема повышения кадрового потенциала является важнейшей и для государственной системы технической защиты информации. Так, в соответствии с постановлениями Правительства Российской Федерации необходимыми требованиями и условиями осуществления лицензируемых видов деятельности в области технической защиты конфиденциальной информации является наличие у специалистов организации-лицензиата, либо соответствующего высшего профессионального образования, либо свидетельства о специальной переподготовке по вопросам защиты информации. Такие требования введены в связи с наличием определенного дефицита квалифицированных кадров по обеспечению безопасности современных информационных технологий.

Органы государственной власти, в частности Федеральная служба безопасности и Федеральная служба по техническому и экспортному контролю Российской Федерации, как компетентные органы всегда уде-

ляли 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 остро ощущается также дефицит и 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 рассматриваемой проблемы, а обсуждаемые вопросы часто не имеют достаточной глубины проработки. Особенно остро данный вопрос стоит при решении проблемы выявления закладочных устройств, предназначенных для получения конфиденциальной информации. Этот вопрос в настоящее время не получил должного освещения в нормативных документах. Положение о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) разрешает ведение этого вида деятельности для своих нужд. В нормативно-методических документах о защите персональных данных также определены угрозы безопасности персональных данных, связанные с перехватом акустической информации с использованием специальных электронных устройств съема речевой информации («закладочных устройств»). Поиск ЗУ должен определяться в соответствии с нормативными документами Федеральной службы безопасности Российской Федерации в установленном порядке, а таких документов пока не существует.

В предлагаемом вниманию читателей специализированном учебном пособии автор, используя существующую литературу, свой опыт работы и методические разработки в данной области, последовательно и в необходимом объеме постарался изложить вопросы, касающиеся организации и осуществления работ по подготовке и проведению работ по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах.

# Введение

Приступая к решению любого вопроса, мы прежде всего интересуемся тем, что же нам известно по данному вопросу, т.е. собираем необходимые данные или информацию. Однако то, что нам представляется важной информацией, другими, не интересующимися данным вопросом, может восприниматься как ничтожный и заурядный шум, поэтому представляется необходимым и актуальным разобраться в том, что же означает термин «информация» и как его трактуют руководящие документы.

В Большой Советской энциклопедии этот термин трактуется следующим образом: «Информация (от лат. informatio — разъяснение, изложение) — сведения, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом (например, с помощью условных сигналов, с использованием технических средств и т.д.), а также сам процесс передачи или получения этих сведений» (БСЭ, издание III, том 10, с. 353).

Федеральный закон № 149 «Об информации, информационных технологиях и защите информации», принятый Государственной Думой 27 июля 2006 г., таким образом трактует это понятие: информация — сведения (сообщения, данные) независимо от формы их представления.

Расширим и уточним, применительно к нашей тематике, понятие информации. Для удобства изложения разделим всю информацию на две основных категории: информация вербальная и невербальная.

Вербальная информация — это различные сведения, выраженные средствами языка (письменно или устно).

Невербальная информация не передает какого-то конкретного содержания, но косвенно указывает, подтверждает или опровергает тот или иной факт. Это перемещения, встречи с кем-то, посещаемые места, поведение и т.д. (например, тайная встреча с представителем конкурирующей фирмы).

Обе категории информации подразделяются на два вида: первый — это (используя американскую терминологию) «мягкая» информация, т.е. информация, носителем которой является поле (акустическое или электромагнитное). Такая информация живет буквально мгновения; однажды произведенная (озвученная), она исчезает и повторно воспроизведена быть не может. Говоря простым языком, «мягкая» информация — это сведения, которые содержатся в произнесенных вами (по телефону или в личной беседе) словах, или ваши текущие действия.

Вторая группа — это «твердая» информация, т.е. информация, записанная на каком-то материальном носителе (бумаге, магнитной ленте и т.п.). Такая информация, если ее специально не стирать, может существовать до тех пор, пока существует сам носитель. К ней можно

отности различные документы, магнитные, кино- и видеозаписи и т.п.

Кроме того, информацию можно условно подразделить:

- на общую или тотальную, которая позволяет получить общее обзорное представление об интересующей проблеме и участниках (индивидах и организациях), решающих данную проблему;
- текущую или оперативную, позволяющую постоянно ориентироваться в курсе изменяющихся событий;
- конкретную, т.е. информацию, позволяющую ответить на определенные вопросы и заполнить выявленные пробелы в имеющихся данных;
- косвенную, которая будучи состыкованной с имеющимися данными по решаемой проблеме только опосредованно, позволяет подтвердить или опровергнуть некие предположения;
- оценочную, позволяющую разобраться и оценить события и дать прогноз относительно их развития в будущем. Это — оптимально обработанные данные.

При этом следует конкретно различать и не путать факты (данные), мнения (личностные предположения) и собственно информацию (аналитически обработанные данные).

Своевременно полученная и достоверная информация обычно позволяет:

- ориентироваться в ситуации;
- четко планировать свои действия;
- отслеживать результативность проводимых акций;
- уклоняться от неожиданностей;
- манипулировать отдельными людьми и группировками.

При этом для получения необходимой информации широко используются ее физические свойства. Следовательно, знание особенностей функционирования информации различного вида позволит успешно организовать защиту от ее утечки по различным каналам. Что же мы подразумеваем под утечкой информации? Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Понятие «утечка» широко распространено. Говорят об утечке воды, газа, материальных ценностей со склада, информации и т.д.

Утечка информации возможна при ее разглашении людьми, утерей ими носителей с информацией, переносом информации с помощью любого вида носителя.

Рассматривая вопрос об особенностях утечки информации, необходимо отметить, что:

- утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику), в отличие, например, от утечки воды или газа;
- при утечке информации происходит ее тиражирование, которое не изменяет характеристики носителя информации (не уменьшается

количество листов документа, не сокращается число пикселей изображения, не меняются размеры, цвет и другие характерные признаки продукции и т.д.);

- цена информации при ее утечке уменьшается за счет тиражирования;
- факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям, когда меры по обеспечению ее безопасности могут оказаться неэффективными.

Следовательно, под утечкой информации следует понимать не процесс распространения носителя информации за пределы определенной области пространства вообще, а частный случай распространения, когда она попадает к злоумышленнику.

Замечание о несанкционированности получателя имеет принципиальное значение. Если получатель информации санкционирован, то речь идет не об утечке, а о передаче информации по так называемому функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.

Современный деловой человек не может отмахиваться от проблем доступа к закрытой информации и сокрытия своей информации. Естественно, не рекомендуется использовать криминальные пути достижения своих целей — заниматься шпионажем для шантажа и вторжения в личную жизнь граждан. Но обязательно необходимо представлять, как это могут сделать другие по отношению к вам.

Обладание одной и той же информацией различными пользователями может привести к абсолютно противоположным результатам. Информацию принято считать ценной лишь тогда, когда ее можно использовать, причем полезность информации сильно зависит от ее полноты, точности и своевременности.

По мнению западных аналитиков, утечка 20 % коммерческой информации в шестидесяти случаях из ста приводит к банкротству фирмы. Информация — второй, после времени, по ценности товар. Кто владеет информацией, тот добивается наибольших результатов.

Для уменьшения угроз экономической деятельности фирмы необходимо получение информации о внешней и внутренней среде, а это включает в себя, помимо прочего, информацию о конкурентах, сотрудниках. Поэтому вполне естественно, что уменьшение данных угроз для одних влечет за собой увеличение угроз экономической деятельности для других.

Получение даже незначительной информации о конкуренте может сэкономить фирме огромные средства, что является достаточно сильным стимулом для нарушения законов, регулирующих отношения в области информации. Сложнее приходится добросовестному субъекту данных отношений, так как он ограничен в своих действиях Законом.

Поэтому знание того, каким путем важная для него информация ограниченного пользования может попасть к конкурентам, позволит собственнику информации организовать ее успешную защиту.

# Оглавление

<b>Введение .....</b>	<b>3</b>
<b>Предисловие .....</b>	<b>5</b>
<b>1. Характеристики технических каналов утечки .....</b>	<b>8</b>
1.1. Общая характеристика каналов утечки информации .....	8
1.1.1. Основные акустические параметры речевых сигналов .....	11
1.1.2. Распространение акустических сигналов в помещениях и строительных конструкциях .....	13
1.1.3. Каналы утечки речевой информации .....	13
1.2. Потенциально возможные технические каналы утечки информации .....	21
1.2.1. Технические каналы утечки речевой информации .....	22
1.2.2. Технические каналы утечки вибрационной информации .....	28
1.2.3. Канал побочных электромагнитных излучений и наводок (разведка ПЭМИН) .....	28
1.2.4. Технические каналы утечки видовой информации .....	31
1.2.5. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники .....	32
1.3. Закладочные устройства и защита информации от них ....	34
1.3.1. Построение и общие характеристики закладочных устройств ..	34
1.3.2. Радиозакладочные устройства .....	36
1.3.3. Радиозакладочные переизлучающие устройства .....	41
1.3.4. Закладочные устройства типа «длинное ухо» .....	42
1.3.5. Сетевые закладочные устройства .....	43
1.3.6. Диктофоны .....	45
1.3.7. Сотовые телефоны .....	48
1.3.8. Направления защиты информации от «легальных» закладочных устройств .....	61
<b>2. Организационно-методические основы защиты информации .....</b>	<b>67</b>
2.1. Общие требования к защите информации .....	67
2.2. Руководящие и нормативно-методические документы, регламентирующие деятельность в области защиты информации .....	70
2.3. Методика принятия решения на защиту от утечки информации в организации .....	75
2.3.1. Алгоритм принятия решения .....	77
2.3.2. Разработка вариантов и выбор оптимального .....	88
<b>3. Организация защиты информации .....</b>	<b>93</b>
3.1. Основные методы инженерно-технической защиты информации .....	93
3.2. Основы подготовки и проведения комплексных проверок ..	95



3.2.1. Принципы проведения комплексных специальных проверок....	96
3.2.2. Подготовительный этап.....	96
3.2.3. Проведение комплексной специальной проверки помещений...	125
3.2.4. Заключительный этап проверки.....	150
<b>4. Приборы и средства обнаружения утечки информации ...</b>	<b>158</b>
4.1. Средства обнаружения каналов утечки информации .....	158
4.1.1. Индикаторы электромагнитных излучений .....	158
4.1.2. Радиоприемные устройства.....	165
4.1.3. Автоматизированные поисковые комплексы .....	173
4.1.4. Принципы функционирования комплексов.....	174
4.1.5. Специальное программное обеспечение.....	176
4.1.6. Специализированные поисковые программно-аппаратные комплексы .....	181
4.1.7. Мобильные поисковые комплексы.....	184
4.1.8. Стационарные комплексы автоматического обнаружения радиомикрофонов .....	188
4.2. Нелинейные локаторы.....	196
4.2.1. Принцип работы нелинейного локатора .....	196
4.2.2. Эксплуатационно-технические характеристики локаторов .....	197
4.3. Досмотровая техника.....	204
4.4. Приборы рентгеновизуального контроля .....	206
4.5. Тепловизионные приборы .....	211
4.6. Эндоскопы .....	214
4.7. Средства радиационного контроля.....	216
Приложения.....	222
Вариант плана проведения комплексной специальной проверки помещений.....	222
Вариант акта проведения комплексной специальной проверки помещений.....	227
Литература.....	230