МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПУТЕЙ СООБЩЕНИЯ (МИИТ)

Кафедра «Организация и технология защиты информации»

П. П. ШАПОВАЛОВ

ПОИСК И ОПЕРАТИВНОЕ ПРЕСЕЧЕНИЕ НЕСАНКЦИОНИРОВАННОГО СЪЁМА ИНФОРМАЦИИ

Рекомендовано
Учебно-методическим объединением вузов
Российской Федерации по образованию
в области историко-архивоведения
в качестве учебного пособия
для студентов высших учебных заведений,
обучающихся по специальностям
090103 «Организация и технология защиты информации»,
090104 «Комплексная защита объектов информатизации»

МОСКВА–2010

УДК 004
Ш 24

Шаповалов П.П. Поиск и оперативное пресечение несанкционированного съема информации: Учебное пособие.- М.: МИИТ, 2010.- 106 с. В учебном пособии подробно методически рассмотрены все этапы проведения работ по поиску элементов и устройств несанкционированного съема и передачи сигналов информации, а также рассматривается пресечение возможных путей утечки информации.

Учебное пособие рассчитано на широкий круг студентов, инженеров, предпринимателей и руководителей служб безопасности организаций с различными формами собственности.

Оно может служить учебным пособием для студентов и преподавателей по учебным дисциплинам "Защита информации", "Основы зашиты информации" и "Техническая зашита информации" для университетов, академий, институтов и колледжей.

Рецензенты;
доктор технических наук, профессор В. Б. Кравченко (Российский государственный гуманитарный университет)
кандидат технических наук, профессор Д. Б. Халяпин (Российский государственный гуманитарный университет)

Оглавление

Предисловие

Проблема защиты информации возникла практически на заре человечества. С развитием общественных отношений, появлением частной собственности, государственного строя, борьбой за власть и дальнейшим расширением масштабов человеческой деятельности информация приобретает все большую ценность. Наиболее ценной становится та информация, единоличное обладание которой позволяет ее владельцу получить какой-либо материальный, политический, военный и т.п. выигрыш [1,2].

С переходом на использование для обработки и передачи информации технических средств информация подвергается воздействию различных неблагоприятных процессов: неисправностей и сбоев аппаратуры, ошибок операторов и т.п., которые могут привести к ее разрушению, изменению, потере, а также создать предпосылки для доступа к ней посторонних лиц. С появлением автоматизированных систем и информационно-вычислительных сетей проблема защиты информации приобретает еще большее значение. Это обусловлено следующими факторами: повышением важности и общественной значимости информации, усилением ее влияния на все без исключения стороны общественной жизни; увеличением объемов информации, накапливаемой, хранимой и обрабатываемой с помощью средств вычислительной техники; сосредоточением в единых банках данных информации различного назначения и

принадлежности; расширением круга пользователей, имеющих доступ к ресурсам автоматизированных систем, в том числе к находящимся в них массивам данных; усложнением режимов функционирования технических средств, широким внедрением многопрограммного режима, режима разделения времени и реального времени; автоматизацией межмашинного обмена информацией, в том числе и на большие расстояния; появлением персональных ЭВМ, расширяющих возможности не только пользователя, но и нарушителя; расширением и усложнением телекоммуникационных сетей.

В 1983 году Министерство обороны США выпустило книгу в оранжевой обложке с названием "Критерии оценки надежных компьютерных систем" (Trusted Computer Systems Evaluation Criteria [3], TCSEC), положив тем самым начало систематическому распространению знаний об информационной безопасности за пределами государственных и военных ведомств. Во второй половине 1980-х годов аналогичные по назначению документы были изданы в ряде европейских стран.

В 1992 году в России Государственная техническая комиссия при Президенте РФ издала серию руководящих документов, посвященных проблеме защиты информации от несанкционированного доступа, средств вычислительной техники и автоматизированных систем [4–7], которые явились практически первыми в нашей стране открытыми изданиями, посвященными этой проблеме.

К настоящему времени как в обществе в целом, так и в сфере технологий обработки данных произошли

большие изменения, которые повлияли на саму суть проблемы защиты информации. Индустрия переработки информации достигла невиданного ранее масштаба. Появилась возможность достаточно свободного выхода в глобальные информационно-вычислительные сети (например, Internet) с персонального компьютера. Развитие систем электронной коммерции создало предпосылки для хищений крупных сумм денег. Широко распространились разнообразные программы-вирусы. Появилось большое количество компьютерных злоумышленников, как профессионалов, так и дилетантов, – хакеров и кракеров, занимающихся несанкционированным доступом к данным, нарушением целостности информационных ресурсов и срывом функционирования различных автоматизированных систем и информационных сетей с самыми разнообразными целями.

В печати регулярно сообщается о все новых и новых компьютерных преступлениях в нашей стране и за рубежом. Так, в частности, В.Левин в 1994 году из Санкт-Петербурга проник в автоматизированную систему Ситибанка США и незаконно перевел 2.8 млн долларов на счета своих сообщников в США, Швейцарии, Нидерландах и Израиле. Служба безопасности филиала Инкомбанка России в 1995 году пресекла попытку бухгалтера этого филиала незаконно перевести крупную сумму в валюте на счета своих сообщников. По сообщениям МВД и ФСБ России, в 1993 году была совершена попытка хищения свыше 68 млн руб. путем манипулирования с данными Центрального банка России [8, 9].

Сегодня наблюдается всплеск интереса информационной безопасности, который объясняется, главным образом, интенсификацией процессов информатизации государственных органов, в том числе вооруженных сил, развитием банковского и страхового бизнеса, ростом и развитием крупных коммерческих структур, выходом их на международный уровень, повышением уровня криминогенной обстановки и терроризма и другими факторами. Поэтому проблема защиты информации в ЭВМ и обеспечения безопасности автоматизированных систем и информационно вычислительных сетей находится в центре внимания не только специалистов по разработке и эксплуатации этих систем, но и широкого круга пользователей.

Следует отметить, что в настоящее время в проблеме защиты информации существует два направления, различающихся характером общественных отношений и формой организации: это защита государственного информационного ресурса (в том числе ресурса систем военного назначения) и защита информации независимого сектора экономики [10–13]. Очевидно, что защитные мероприятия призваны обеспечить конфиденциальность, целостность и доступность информации, однако если для режимных государственных организаций на первом месте стоит конфиденциальность, а целостность понимается в основном как неизменность информации, то для коммерческих структур, как правило, важнее всего целостность (актуальность) и доступность данных и услуг по их обработке.

Настоящее учебное пособие посвящено рассмотрению вопросов поиска устройств

несанкционированному съему и пресечению их функционированию. Оно состоит из девяти разделов.

В первом разделе дана классификация возможных вариантов мотиваций поисковых исследований, а также рассмотрены особенности реализации различных мотиваций.

Во втором разделе описано изучение объекта поиска и его окружения, обращая особое внимание на изучение прогнозируемого противника.

Разработке плана поисковых исследований посвящен третий раздел. В разделе рассматривается подготовка к проведению поисковых работ.

Четвёртый раздел посвящен осмотру и проверке предметов быта и интерьера объекта поиска.

В пятом разделе рассмотрен порядок поиска устройств съема информации, внедрённых в электронные приборы, находящиеся на объекте поиска.

Исследование электромагнитной обстановки в помещениях, в автомашинах и на открытой местности рассмотрено в шестом разделе.

Проверка наличия устройств съема информации или их элементов в абонентской и офисной телефонной сети, в электросети, в радиотрансляционной сети, в линиях пожарной и охранной сигнализации рассмотрена в седьмом разделе.

В восьмом разделе рассматриваются поисковые исследования по обследованию стен, потолочных перекрытий, полов, вентиляционных каналов, тепло и водопроводных коммуникаций и других элементов строительных конструкций.

ВВЕДЕНИЕ

Последнее десятилетие 20 века в Российской Федерации установился дикий капитализм, который характеризуется многими негативными процессами. Одним из них является разнузданная добыча конфиденциальной информации* по любым вопросам деятельности организаций различных форм собственности. Об этом свидетельствует множество публикаций на эту тему, появившихся в журналах: "Защита информации", "Технология и средства связи", "Системы безопасности"; в книгах: Хорев А. А. Технические средства и способы промышленного шпионажа [14], Лунегов А.Н., Рыжов А.Л. Технические средства и способы добывания и защиты информации[15], Брусницин Н. А. Открытость и шпионаж. [16], а также во многих газетах и других изданиях.

Примечание. Здесь и в последующем под **конфиденциальной информацией** будем понимать служебную, производственную, организационную, личную и другую информацию, используемую в деятельности организаций различных форм собственности и разглашение которой может привести к материальному или моральному ущербу

Анализ вышеназванных публикаций, а также других открытых публикаций по этой тематике [17-21], показывает, что в настоящее время для несанкционированного съема информации могут быть использованы различные приёмы, такие как:

- подслушивание разговоров в помещениях, в автомашинах и на открытой местности с помощью

- радио, радиотелефонных, телефонных и других устройств связи;
- снятие информации с телефонных и телексных линий связи и их элементов;
- дистанционный съем разговоров в помещениях, в автомашинах и на открытой местности путём направленного радио и лазерного облучения;
- дистанционный съем разговоров с любых объектов заинтересованности, используя направленные микрофоны;
- дистанционный приём побочных электромагнитных излучений, формируемых ПК, компьютерными сетями, печатающей и множительной техникой и другой аппаратурой;
- негласное использование видео и фотоаппаратуры.

Примечание. Здесь и в последующем под **объектом заинтересованности** будем понимать помещение, автомашина и открытая местность (парк, зона отдыха, сквер и т.д.), из которых может осуществляться добыча информации.

Следует отметить, что каждый из вышеописанных приёмов несанкционированной добычи информации, практически, может быть реализован несколькими способами.

Многообразию приёмов, способов и практической реализации несанкционированной добычи конфиденциальной информации должны противодействовать продуманные организационные, технические и организационно-технические мероприятия.

Как показано в работе [19], для предотвращения утечки информации владельцы информации должны

проводить свою работу по следующим трём направлениям:

-организационные мероприятия, заключающиеся в создании условий, обеспечивающих невозможность несанкционированно добыть информацию на всех стадиях её функционирования (формирования, преобразования, передачи её из одного места в другое и хранения);

-технические мероприятия, позволяющие осуществить фиксацию, блокировку или нейтрализацию функционирования; устройств съема информации* и передачи их по всем возможным каналам утечки информации;

-поисковые мероприятия, позволяющие, вер-первых; определить наличие в том или ином месте устройств несанкционированного съема информации и пресечь их функционирование; во-вторых, оценить потенциально возможные каналы утечки информации и предложить пути их нейтрализации.

Примечание. В последующем устройства и системы несанкционированного съема информации с объекта заинтересованности и передача её на стационарный или мобильный пункт приёма по любым каналам связи будем называть **устройства съема информации,** а мероприятия, направленные на поиск устройств съема информации и нейтрализацию их функционирования будем называть **поисковыми исследованиями.**

Только комплексное использование вышеперечисленных мероприятий может свести к минимуму утечки конфиденциальной информации.

Однако, определяющими при комплексном подходе к предотвращению утечки информации

являются поисковые исследования, позволяющие по мере поступления сигнала об утечке информации или сигнала тревоги, указывающего на попытку съема информации, уверено определить наличие или отсутствие на объекте поиска устройств съема информации и оперативно предотвратить их функционирование, а также позволяющие оценить наличие потенциально возможные технические каналы утечки информации.

Примечание. Здесь и в последующем под **объектом поиска** будем понимать помещение, автомашина или открытая местность с имеющимися аппаратурой, предметами быта и интерьера и другими материалами, находящимися в них, в которых проводится поисковые исследования или оцениваются возможные каналы утечки информации

Поисковые исследования могут проводиться на любом объекте поиска как со стационарным, так и с временным внедрением устройств съема информации.

Примечание. Здесь и в последующем под **стационарным внедрением** устройств съема информации будем понимать внедрение элементов, устройств или систем съема информации в элементы строительных конструкций (стены, потолочные перекрытия, пол, окна и т.д.), в проводные коммуникации (абонентскую телефонную сеть, электросеть, радиотрансляционную сеть и т.д.), в предметы быта и интерьера, в салон или в багажник автомобиля или в кусты и в другие места на открытой местности с целью получения информации в течении длительного времени (нескольких месяцев или нескольких годов) функционирования коммерческой организации, а под **временным внедрением устройств** съема информации будем

понимать внедрение, как правило, всего устройства или системы съема информации в целом, осуществляемое путём конспиративного их заноса на объект поиска с целью получения конфиденциальной информации о конкретной деятельности конкурирующей организации в течении ограниченного времени (не более нескольких суток).

Следует отметить, что при стационарном внедрении устройств съема информации их питание осуществляется, как правило, от линии электросети, а при временном внедрении - от автономного источника тока.

Поисковые исследования на любом объекте поиска могут проводиться как комплексно, так и ограниченно по отдельным возможным каналам утечки информации или в отдельных элементах быта и интерьера.

Примечание. Здесь и в последующем под **комплексными поисковыми исследованиями** будем понимать поисковые работы, направленные на отыскание и, при необходимости, предотвращения функционирования или изъятия устройств съема информации, при которых обследуются все возможные каналы утечки информации, а под **ограниченными исследованиями** будем понимать поисковые исследования, направленные на отыскание и, при необходимости предотвращения функционирования или изъятия технических средств съема информации, проводимые в определённых каналах утечки информации.

Как при комплексных, та и при ограниченных поисковых исследованиях работы проводятся для решения основной цели, а именно, определения наличия (отсутствия) устройств съема

информации при любом варианте их внедрения.

Независимо от способа внедрения устройств съема информации и вида поисковых исследований все работы должны проводиться конспиративно, соблюдая по возможности все этапы, которые в обобщенном виде могут состоять из:

- изучения объекта заинтересованности и его окружения;

- визуального осмотра и проверки всех предметов, находящихся на объекте поиска;

- исследования в помещении, в автомашине и на открытой местности на наличие в них радиотехнических устройств съема информации:

- электромагнитного поиска устройств съема информации;

- поиска устройств съема информации в проводных коммуникациях (абонентская телефонная сеть, электросеть, радиотрансляционная сеть, линии пожарной и охранной сигнализации и т.д.);

- изъятия устройств съема информации;

- оценки потенциально возможных каналов утечки конфиденциальной информации.

На каждом вышеописанном этапе поисковых исследований используются те или иные специальные технические средства.

Эффективность поиска устройств съема информации, их изъятие и определение потенциально возможных каналов утечки информации определяется наличием технических средств поиска с требуемыми параметрами, высоким организационно-техническим уровнем проведения поисковых работ на всех этапах их осуществления, а также профессиональным

уровнем участников проводимых исследований.

Подробному описанию всех вышеназванных этапов поисковых исследований с использованием специальных технических средств, разработанных научно - производственной фирмой «Щит» и выпускаемых другими коммерческими организациями посвящено настоящее учебное пособие.

Учебное пособие состоит из девяти разделов

В первом разделе дана классификация возможных вариантов мотиваций поисковых исследований, а также рассмотрены особенности реализации различных мотиваций.

Во втором разделе описано изучение объекта поиска и его окружения, обращая особое внимание на изучение прогнозируемого противника.

Разработке плана поисковых исследований посвящен третий раздел. Кроме того в этом же разделе рассматривается подготовка к проведению поисковых работ.

Четвёртый раздел посвящен осмотру и проверке предметов быта и интерьера объекта поиска.

В пятом разделе рассмотрен порядок поиска устройств съема информации, внедрённых в электронные приборы, находящиеся на объекте поиска.

Исследование электромагнитной обстановки в помещениях, в автомашинах и на открытой местности рассмотрено в шестом разделе.

Проверка наличия устройств съема информации или их элементов в абонентской и офисной телефонной сети, в электросети, в радиотрансляционной сети, в линиях пожарной и охранной сигнализации рассмотрена в седьмом разделе.

В восьмом разделе рассматриваются поисковые исследования по обследованию стен, потолочных перекрытий, полов, вентиляционных каналов, тепло и водопроводных коммуникаций и других элементов строительных конструкций. Подведению итогов поисковых работ посвящен девятый. В приложении 1 и 2 даны образцы краткого описания проведения поисковых исследований.

РАЗДЕЛ 1. МОТИВАЦИИ ПОИСКОВЫХ ИССЛЕДОВАНИЙ И ОСОБЕННОСТИ ИХ РЕАЛИЗАЦИИ.

Как было сказано ранее, поисковые исследования проводятся с целью: во-первых, отыскания устройств съема информации; во-вторых, определения возможных путей утечки информации в любых местах деятельности организации (в помещениях, в автомашинах или на открытой местности) и в третьих, пресечения утечки информации как путём нейтрализации функционирования устройств съема информации, так и путём устранения найденных каналов утечки информации с помощью определённых технических средств и организационных мероприятий.

Поисковые исследования проводятся, как правило, по указанию руководства организации, в основе которых могут реализоваться следующие возможные мотивации:

- утеря конкретных конфиденциальных материалов;

-проявление заинтересованности (конкурирующей) организации к определенным конфиденциальным материалам или к деятельности в целом;

- предупреждающие профилактические действия ;

Примечание. Здесь и в последующем введены следующие сокращения :

- мотивация "утеря конкретных материалов" - **утеря материалов**;

-мотивация "проявление заинтересованности (конкурирующей) организации к определённым

материалам или к коммерческой деятельности в целом"- **проявление заинтересованности**;

- мотивация "предупреждающие профилактические действия" - **профилактика.**

Каждая из вышеназванных мотиваций накладывает определённые требования на объем проводимых поисковых работ на каждом этапе их выполнения, на сроки их выполнения и на конспиративность их осуществления.

Мотивация поисковых исследований "утеря материалов" характеризуется конкретностью утерянной информации (материалов). Это приводит к целенаправленным поискам и сокращает сроки их проведения.

При поисковых исследованиях, основанных на этой мотивации, решаются, как правило, следующие задачи:

- добывается информация об объекте поиска и о прогнозируемом противнике;

- вырабатываются предложения и оперативно практически реализуются мероприятия по предотвращению утечки конфиденциальной информации в процессе проведения поисковых работ;

- оцениваются возможные каналы утечки конфиденциальной информации, возможные способы съема информации и возможные места размещения аппаратуры приёма и обработки информации;

- определяются конкретные места возможного размещения устройств съема информации;

- отыскиваются устройства съема информации;

- изымаются из мест внедрения, если есть указания;

Руководства организации объекта поиска, отдельные элементы, устройство или система съема информации в

целом;

- восстанавливается по указанию руководства организации объекта поиска функционирование системы съема информации, которая может быть использована в последующем в качестве устройств дезинформации предполагаемого конкурента;

-разрабатываются предложения по нейтрализации в последующем возможных устройств съема информации.

Примечание. В последующем организация, которая, как предполагают руководители объекта поиска, осуществляет несанкционированную добычу конфиденциальной информации, будем называть **прогнозируемым противником.**

При решении вышепоставленных задач на начальном этапе их выполнения особое внимание уделяется добыче необходимой информации, позволяющей спрогнозировать, а лучше всего определить прогнозируемого противника, несанкционированно добывающего конфиденциальные материалы, его профессиональные и технические возможности. Эта исходная информация является основой для разработки плана конспирации, проведения поиска и его осуществления, обращая особое внимание на конспирацию проводимых работ и на выработку легенды и её реализации в процессе проведения поисковых работ на всех этапах их реализации.

Следует отметить, что прогнозируемым противником может быть не одна, а несколько разных взаимосвязанных конкурирующих организаций или группа сотрудников, нанятых конкурирующей организацией, как правило, обладающие высоким профессиональным уровнем и имеющие самые

разнообразные технические средства, позволяющие конспиративно добыть, практически, любую информацию, использую различные каналы связи.

Добыча информации в процессе проведения поисковых работ, в том числе и о прогнозируемом противнике, может осуществляться гласно или негласно, используя следующие приёмы:

- гласные или замаскированные опросы своих сотрудников и сотрудников других организаций, имеющих прямое или косвенное отношение к опросной тематике;

- изучение протоколов, отчетов, докладов, накладных, договоров, образцов продукции и т. д., обращая особое внимание на сведения прямо или косвенно связанные с утерянной информацией;

- изучение по возможности аналогичных информационных материалов прогнозируемого противника;

- изучение и анализ всех материалов, имеющих отношение к нарушению ведения делопроизводства в том числе и к прохождению всех утерянных конфиденциальных материалов как внутри офиса, так и за его пределами;

- изучение материалов, относящихся к нарушению режима посещения офиса своими и посторонними сотрудниками.

Информация в процессе поисковых исследований может добываться, используя технические и интеллектуальные каналы как внутри организации объекта поиска, так и за её пределами с обязательным соблюдением всех элементов конспирации.

После анализа полученной информации

определяется или очерчивается круг вероятного "противника", оцениваются его потенциальные профессиональные, а также оперативные и технические возможности по добыче информации и по её защите, на основании которых разрабатывается план поисковых исследований, который, в зависимости от сложности и объема выполняемых работ, может быть представлен в устной или письменной форме.

Для проведения поисковых исследований, базирующихся на мотивации "утеря материалов", должны быть предусмотрены следующие виды работ:

- визуальный осмотр и проверка всех предметов быта и интерьера, находящихся на объекте поиска, на наличие в них устройств съема и передачи сигналов информации;

- поиск устройств съема и передачи сигналов информации, внедренных в электронные приборы;

- исследование электромагнитной обстановки на объекте поиска;

- проверка проводных коммуникаций (абонентской телефонной сети, электросети, радиотрансляционной сети, линии пожарной и охранной сигнализации и т.д.) на наличие в них устройств съема информации.

Объем каждой работы и сложность их выполнения зависит от конкретной утерянной информации.

Первые три вида работ в поисковых исследованиях, базирующихся на первой мотивации, проводятся всегда.

Проверка проводных коммуникаций, ввиду её сложности и необходимости большого времени для её выполнения, применяется при явном определении на начальной стадии уровня поисковых исследований,

при использовании прогнозируемым противником для передачи негласно снятых сигналов информации той или иной проводной коммуникации или при отсутствии положительного эффекта в первых трёх видах работ и при наличии необходимого времени.

Учитывая, что поисковые исследования, реализующие мотивацию "утеря материалов", как правило, ограничены по времени, поэтому отдельные виды работ могут выполняться не в полном объеме (объем проводимых работ всегда должен быть согласован с руководителем организации объекта поиска) и, в следствии этого, к сожалению, не всегда проведения поисковых работ выполняются конспиративно.

Поисковые исследования, основанные на мотивации "проявление заинтересованности", проводятся с целью: во-первых, отыскания возможных устройств съема информации; во-вторых, определения возможных каналов утечки информации; в- третьих, создания организационных и технических условий, преграждающих утечку информации.

Особое внимание на начальном этапе этих исследований необходимо уделить изучению и конкретизации как имеющихся конфиденциальных материалов, так и направлениям деятельности организации поиска, которые могут представлять интерес для конкурирующих организаций.

На основании полученных материалов прогнозируются возможные каналы утечки информации и разрабатывается план проведения поисковых исследований.

Также, как и при разработке плана поисковых исследований, реализующих, рассмотренную ранее

мотивацию "утеря материалов", при разработке плана поисковых исследований, для реализации мотивации «проявления заинтересованности» используется гласная и негласная добыча материалов по всем возможным направлениям.

Отличительной особенностью в добыче материалов при реализации мотивации "проявление заинтересованности" является широта и разнообразие добываемых материалов, для чего может быть привлечено большое количество сотрудников, которые прямо или косвенно имели или имеют отношение к какой либо части или ко всем конфиденциальным материалам. Для добычи этих материалов, как правило, требуется большое время.

Вышеперечисленная особенность в подготовке материалов для разработки плана поисковых исследований, накладывает жесткие требования на конспиративность их добычи, а также на конспиративность проведения поисковых исследований на всех этапах их осуществления.

Поисковые исследования, реализующие эту мотивацию, характеризуются не только широтой добываемой информации на подготовительном этапе, но и многообразием видов работ, проводимых в процессе поисковых исследований, требующих большое время для их реализации.

В обобщенном виде поисковые исследования, реализующие эту мотивацию, имеют такой же набор работ, что и поисковые исследования, реализующие мотивацию "утеря материалов".

Следует отметить, что на момент начала поисковых исследований на объекте поиска желательно, чтобы поисковой бригаде были известны все характерные особенности места их проведения

(помещение, автомашина, открытая местность).

Независимо от объема поисковых работ они всегда должны проводиться по заранее разработанному плану, в котором расписаны все виды работ, место и время их проведения, участники работ, оперативное их обеспечение, используемая аппаратура и её потребительские параметры и другие моменты, специфичные для конкретного поискового исследования .

Для наиболее значимых комплексных поисковых исследований, как правило, разрабатывается план конспирации проведения работ отдельно.

План поисковых исследований, реализующих эту мотивацию и план конспирации их проведения целесообразно подготавливать в письменном виде.

В связи с большим объемом работ в поисковых исследованиях, наряду с поисковой бригадой, могут принимать участие также и сотрудники организации, имеющие непосредственное отношение к службе безопасности. Они привлекаются к выполнению отдельных вспомогательных работ.

Руководство поисковыми исследованиями на всех этапах их реализации осуществляет старший поисковой бригады, имеющий большой профессиональный опыт проведения аналогичных работ.

Для проведения поисковых исследований должно быть достаточное время для выполнения их на хорошем оперативно-техническом уровне.

Широта, глубина и достаточное время для проведения поисковых исследований позволяет: во-первых, подтвердить наличие или отсутствие канала утéчки информации; во-вторых, обнаружить или не обнаружить устройство съема и передачи негласно

снимаемой информации; в-третьих, оценить надёжность (ненадёжность) информационной защиты и выработать, если это необходимо, меры по обеспечению интеллектуальной и технической защиты информации.

Поисковые исследования, основанные на мотивации "профилактика", проводятся поисковой бригадой или, в некоторых случаях, сотрудниками службы безопасности объекта поиска с целью проверки надёжности обеспечения сохранности конфиденциальной информации и материалов.

Проведение этих поисковых исследований осуществляется, как правило, по заранее разработанному графику, в который могут быть включены как комплексные, так и ограниченные поисковые исследования.

График проведения профилактических поисковых исследований подготавливается заранее. С ним могут быть ознакомлены только руководитель организации, отвечающий за информационную безопасность, и руководитель службы безопасности.

Профилактические поисковые исследования, независимо от объема работ проводятся по детально разработанному плану, в котором отражается место, время, объем, участники проводимых работ, используемая аппаратура и оперативное и техническое их обеспечение и другие необходимые моменты. Независимо от объема проводимых работ особое внимание в плане поисковых исследований должно быть уделено вопросу конспирации на всех этапах их осуществления.

План профилактических поисковых исследований чаще всего оформляется в письменном виде.

Одним из важных условий успешного проведения поисковых исследований, независимо от их мотивации, является обеспечение конспирации и легендирования выполнения всех работ на всех этапах их осуществления.

Следует отметить, что конспиративность и легендирование проведения поисковых исследований неукоснительно должны выполняться независимо от объема и складывающихся условий их осуществления.

С целью чёткого обеспечения конспирации проведения поисковых работ на подготовительном этапе, если имеется такая возможность, должен быть разработан подробный план по конспирации и легендированию проводимых работ с обязательным указанием документов и материалов прикрытия.

В планах по обеспечению конспирации проведения поисковых работ особое внимание должно быть уделено легендированию. С этой целью на каждый вид работ и на всю работу в целом должны быть разработаны легенды, которые естественно должны вписываться в деятельность организации. Легенды должны подтверждаться необходимыми материалами и документами прикрытия, а также приборами и инструментами.

В качестве легенд можно рекомендовать:

-проверка функционирования сетей связи на объекте поиска и его окружения (мобильная радиотелефонная связь, абонентская и офисная телефонная связь и т.д.):

-проверка функционирования пожарной и охранной сигнализации:

-оценка электроизоляции линии электросети:

-измерение электромагнитной и радиационной

обстановки на объекте поиска и его окружения:

-оценка износостойкости и коррозийности автомобиля, мотоцикла и других средств передвижения :

-проведение ремонтных работ машины;

-проведение косметического ремонта помещения:

-проверка санитарного состояния помещения;

Наряду с этим в процессе проведения поисковых исследований могут быть использованы и другие легенды, которые должны естественно вписываться в условия их осуществления.

Следует отметить, что в некоторых случаях проведение поисковых исследований может быть осуществлено без легендирования. т. е. до сотрудников, не участвующим в проведении исследований доводится информации о том, что в офисе проводятся работы по поиску устройств съема информации.

Для каждой из вышеназванных легенд, а также для других легенд, которые могут быть использованы в процессе поисковых исследований, как было сказано ранее, должны быть предложены определенные документы прикрытия, сопутствующие приборы и материалы, которые естественно вписываются в проводимые работы.

Кроме этого в процессе выполнения легенд каждый сотрудник поисковой бригады должен

демонстрировать те навыки и умения, которые естественно вписываются в выбранную легенду. С этой целью на подготовительном этапе после формирования легенды сотрудники поисковой бригады должны формировать навыки и умения,

которые позволят конспиративно провести все поисковые работы на всех этапах их осуществления.

Выбор той или иной легенды, документов прикрытия и сопутствующих приборов и материалов зависит в первую очередь от мотивации проведения поисковых работ, а также от сложившихся условий на объекте поиска.

Следует напомнить, что все виды поисковых работ должны выполняться в соответствии с разработанными легендами, ибо невыполнение их может привести к срыву проведения отдельных видов работ или всей работы в целом, а в некоторых случаях даже к криминальным действиям со стороны прогнозируемою противника или его "доверенных" организаций.

Как было сказано ранее, при разработке плана поисковых исследований должен быть разработан план конспирации, который может быть представлен или в виде раздела в плане поисковых работ или в виде самостоятельного плана. Также как и план поисковых исследований, план конспирации в зависимости от вида мотивации, объёма работ и имеющегося времени может быть представлен в устном или письменном виде.

При проведении поисковых исследований, реализующих мотивацию "утеря материалов", как правило, план по обеспечению конспирации проведения работ представляется в устном виде, а для поисковых исследований, реализующих мотивации "проявление заинтересованности" и "профилактика" план целесообразно представлять в письменном виде.

РАЗДЕЛ 2. ИЗУЧЕНИЕ ОБЬЕКТА ПОИСКА И ЕГО ОКРУЖЕНИЯ

Изучение объекта поиска и его окружения, как было сказано ранее, является основой поисковых исследований, так как материалы полученные на этом этапе определяют тактику проведения поисковых исследований, объем и результативность проведенных работ и конспиративность их осуществления, что в конечном счёте также является залогом их результативности.

Одним из важных вопросов в изучении объекта поиска и ею окружения является добыча материалов о вероятном противнике, а в некоторых случаях о нескольких противниках, его (их) профессиональных и технических возможностях.

Добыча материалов о вероятном противнике должна начинаться с подробного расспроса у руководителя организации объекта поиска, а также у руководителя службы безопасности о мотивации проведения поисковых исследований, о конкретных причинах приглашения поисковой бригады и о возможной причастности прогнозируемого противника к указанной мотивации.

После расспроса руководителя организации и руководителя службы безопасности объекта поиска и анализа полученных от них материалов ведущие сотрудники поисковой бригады проводят сверку их с фактическими материалами, которые добываются путём предварительного анализа предполагаемых каналов утечки информации и путём проведения по возможности совместно с сотрудниками организации

объекта поиска мероприятий, направленных на добычу информации о технических и профессиональных возможностях прогнозируемого противника.

На основании полученной информации руководитель поисковой бригады уточняет прогнозируемого противника, его технические и профессиональные возможности и обсуждает полученные материалы с руководством организации.

Особое место в изучении объекта поиска и его окружения занимает сбор информации по ведению делопроизводства на объекте поиска, по порядку прохождения конфиденциальной информации как внутри организации объекта поиска, так и за её пределами, по режиму работы организации и посещения ее посторонними сотрудниками, в том числе и возможного посещения сотрудниками прогнозируемого противника, по взаимодействию между сотрудниками внутри организации и с сотрудниками других организаций и по другим вопросам, способствующие оперативно, скрытно и эффективно провести поисковые исследования.

На данном этапе поисковых исследований также необходимо уделить определенное внимание изучению застройки местности, планировки помещений, расстановки мебели. предметов быта и интерьера, наличию особенностей местности, зданий и ограждающих конструкций, состоянию обивки салона автомобиля, кресел, стульев и других предметов, находящихся на объекте поиска.

Здесь также изучается порядок проведения косметического и капитального ремонтов помещений, монтажа и демонтажа проводных и

трубопроводных коммуникаций, замены мебели, перестановки предметов быта и интерьера.

Кроме этого изучаются факты получения сувениров, подарков и других предметов от сотрудников других организаций, а также изучается покупка мебели, картин, радиоаппаратуры и т. д.

Следует отметить, что добыча необходимой информации и материалов может осуществляться как конспиративно, так и де конспиративно.

Что касается информации и материалов по прогнозируемому противнику то они добываются конспиративно и только в исключительных случаях они добываются без соблюдения конспирации.

Добыча информации и материалов в процессе изучения объекта поиска и его окружения как конспиративно, так деконспиративно должна осуществляться конфиденциально по возможности с привлечением ограниченным кругом лиц, что позволит путём сравнения информации, полученной от разных источников, объективно добыть достоверную информацию по всем вопросам, касающимся объекта поиска и его окружения, но и о прогнозируемом противнике и его технических и профессиональных возможностях.

В зависимости от полученной информации и особенно от информации касающейся прогнозируемого противника, его технического и профессионального состояния, от его намерения добывать информацию "одноразовой" конфиденциальной информации или многократное её получение, направленность работ поисковой \ бригады должна быть нацелена:

- на обнаружение устройств съема

информации, закамуфлированных в какие-либо предметы быта и интерьера, в радио, теле и другую аппаратуру, в элементы проводных коммуникаций и в другие предметы, которые могут быть внесены на объект поиска с обеспечением от автономного источника тока (батареи или аккумуляторы), а в некоторых случаях с обеспечением питания от линии электросети или телефонной линии;

-на обнаружение устройств съема информации стационарно внедренных в элементы строительных конструкций (стены, пол, потолочные перекрытия, вентиляционный канал и т.д.), в элементы абонентской телефонной сети (телефон, розетку, телефонный шкаф и т.д.), в электросеть (розетка, подрозетник и т.д.) и в элементы других проводных коммуникаций, а также в элементы предмета быта и интерьера с обеспечением их питания от линии электросети.

Следует отметить, что при "одноразовой" добыче конфиденциальной информации наиболее вероятным каналом передачи негласно добытой информации является радиоканал. В этом случае питание устройства съема информации, как правило, осуществляется от автономного источника тока (батареи или аккумулятора).

При "многократной" добыче информации, как правило, осуществляется стационарное внедрение на объекте заинтересованности устройств съема информации, а в качестве канала передачи сигналов информации может быть использована закамуфлировано проложенная проводная линия, абонентская телефонная линия, линия электросети и другие проводные коммуникации.

Питание таких устройств съема информации, чаще всего, осуществляется от электросети.

Наряду с этим в качестве каналов передачи сигналов информации, как указано в работе [19], могут быть элементы строительных конструкций (пол, стены, потолочные перекрытия, водопроводные трубы, оконные стекла и т.д.). В этом случае устройства съема информации, в основном, размещаются на пункте приёма и обработки сигналов, который, как правило, устанавливается за пределами помещений объекта поиска.

Вышеперечисленные особенности при "одноразовой' и "многократной" негласной добыче информации должны быть учтены при изучении объекта поиска и его

окружения.

Добытая информация в результате изучения объекта поиска и его окружения должна быть достаточной для:

-формирования моделей возможных вариантов съема и передачи конфиденциальной информации;

- определения возможных способов внедрения устройств съема информации;

-определения возможных каналов передачи сигналов информации;

-определения мест возможного внедрения устройств съема информации и мест размещения аппаратуры пункта приёма и обработки информации;

-выработки наиболее приемлемых путей поиска устройств съема информации и изъятия их из мест внедрения;

-формирования тактики поиска устройств информации и разработки вариантов их

функционирования.

В процессе изучения объекта поиска и его окружения но возможности должна быть:

-подготовлена планировка местности, планировка всех помещений организации объекта поиска, схема проводных, водо и теплопроводных коммуникаций;

-осуществлена опись материалов ограждающих конструкций;

-составлен список приборов, устройств, инструментов и материалов, которые могут быть использованы в процессе поиска и изъятия устройств съема информации.

Эти материалы являются основой для подготовки плана проведения поисковых работ, плана конспирации и плана легендирования их осуществления.

РАЗДЕЛ 3. РАЗРАБОТКА ПЛАНА ПОИСКОВЫХ ИССЛЕДОВАНИЙ И ПОДГОТОВКА К ИХ ПРОВЕДЕНИЮ

На основании информации и материалов, полученных в процессе изучения объекта поиска и его окружения, их анализа и обобщения разрабатывается план проведения поисковых исследований, который, как было сказано ранее, может быть представлен в письменном или устном виде.

При подготовке плана проведения поисковых исследований необходимо определить содержание работы на каждом этапе их осуществления с указанием перечня необходимой аппаратуры, инструментов и материалов и разработать меры по обеспечению конспирации их выполнения.

Как было сказано ранее, в обобщенном виде для выполнения комплексных поисковых исследований в полном объеме необходимо запланировать следующие виды работ.

В первом виде работ поисковых исследований осуществляется визуальный осмотр предметов быта и интерьера, сувениров, папок, мебели, аппаратуры и других предметов, находящихся на объекте поиска и в помещениях прилегающих к нему. Для осуществления эффективного визуального осмотра необходимо подготовить и проверить функционирование металлоискателя, досмотровое зеркало с подсветкой, набор луп с различным увеличением, электрический фонарь, набор монтажника, состоящего из мультитестера, паяльника, ,набора отверток, пинцета, плоскогубцы, резиновый молоток и другие изделия.

Во втором виде работ поисковых исследований проводится проверка электронных приборов, радио и видеоаппаратуры и оргтехники на наличие в них элементов устройства съема информации или же на наличие канала утечки информации, образующегося в них.

В этом случае необходимо иметь набор технических средств, который используется при проведении первого вида работ, также комплекс радио мониторинга и копии фотографий монтажных схем электронных приборов и радио и видеоаппаратуры, телефонных аппаратов, телефакса, ксерокса и другой аппаратуры, находящейся на объекте поиска и позволяющие осуществить разборку, визуальный осмотр и сравнение с фотографией расположение радиоэлементов в анализируемом приборе.

В третьем виде поисковых работ осуществляется разборка, если такая возможность имеется, и визуальный осмотр элементов электросети (розеток, выключателей, удлинителей и т.д.), абонентской телефонной сети, (телефонных аппаратов, розеток, распределительных коробок, плинтов и т.д.), линии пожарной и охранной сигнализации (датчиков, коммутаторов и т.д.), радиотрансляционной сети (радиоприёмник, вилка, розетка, выключатели и т.д.) и других имеющихся на объекте поиска средств связи. Для выполнения этого вида поисковых работ необходим набор инструментов и набор луп с различным увеличением.

Четвёртый вид поисковых работ посвящен исследованию и анализу электромагнитной обстановки в помещениях, в автомашинах и других местах объекта поиска и его окружения.

Для исследования электромагнитной обстановки и его окружения необходимо подготовить комплекс радио мониторинга, выполненный на базе сканирующего радиоприёмника. Этот комплекс должен обеспечивать прием и обработку спектральных составляющих радиосигналов в ручном и автоматическом режимах в диапазоне частот 100 кГц до 1,5 ГГц, а также должна осуществляться запись их и сравнение полученных результатов с имеющимися в компьютере усредненных или спектральных составляющих радиоизлучении, измеренных на других объектах поиска.

В пятом виде поисковых работ исследуются имеющиеся на объекте поиска проводные коммуникации (электросеть, абонентская[1] телефонная сеть, радиотрансляционная есть, селекторная линия связи, сеть персонального вызова и диспетчерской связи и т.д.) на наличие в них сигналов устройств съема информации, а также на наличие в них каналов утечки информации.

Для проведения этого вида работ необходимо иметь набор инструментов, тестер, усилитель низкой частоты с головными телефонами и блоком сопряжения, обеспечивающие согласования их параметров с параметрами различных проводных коммуникаций, осциллограф и комплекс поиска и обнаружения сигналов устройств съема информации в проводных коммуникациях.

Шестой вид поисковых работ направлен на поиск и обнаружение устройств съема информации в элементах строительных конструкций (в стенах, в полу, в потолочных перекрытиях, в окнах и т. д.), а в некоторых случаях, и их изъятие. Для обследования элементов строительных конструкций необходимы металлоискатель, нелинейный локатор, набор луп,

набор инструментов, отпариватель обоев и другие материалы, которые обеспечивают не только определение мест размещения элементов устройств съема информации в любом месте, но и их изъятие на глубине их размещения.

На стадии добычи исходной информации руководитель организации поисковой бригады должен:

-установить контакт с руководителем организации объекта поиска или лицом ответственным за безопасность в ней;

-разработать легенду своего появления па предполагаемом объекте поиска, которая в последующем должна по возможности естественно вписываться в легенду проведения поисковых исследований;

-принять участие в разработке и согласования плана проведения поисковых исследований;

-разработать и согласовать план оперативного обеспечения проводимых работ;

-решить вопрос доставки и хранения аппаратуры;

Исходя из профессионального уровня прогнозируемого "противника", его технической оснащённости и особенностей объекта поиска для каждого вида работ должны быть смоделированы возможные варианты их выполнения, а также должны быть определены и подобраны набор аппаратуры, инструментов и материалов.

После намеченных видов работ определяется последовательность и сроки их проведения.

Следует отметить, что в зависимости от объема работ, необходимого времени, имеющихся условий на

объекте поиска и его окружения и необходимого количества людей поисковой бригады в плане поисковых исследований может быть запланировано параллельное или последовательное выполнение отдельных видов работ.

В плане необходимо предусмотреть возможность удаления из помещений в которых проводятся поисковые исследования сотрудников организации объекта поиска, в том числе и руководителей, не участвующих в поисковых исследованиях, ибо, чем меньше людей будут ознакомлены с методикой их проведения и поисковой техникой, тем более успешно они могут быть проведены. Как правило, в поисковых исследованиях принимают участие от организации объекта поиска один, максимум два человека.

Особое внимание при подготовке плана поисковых исследований должно быть уделено анализу возможных работ в подозрительных и наиболее вероятных местах возможного размещения элементов устройств съема информации, как с точки тщательности проведения работ в этих местах (поиск в этих местах должен проводиться высокопрофессиональными сотрудниками и с использованием различных методов и аппаратуры), так и с точки зрения конспиративности их осуществления.

Наряду с этим в плане должны быть запланированы действия бригады в случае обнаружение устройств съема информации или канала утечки информации.

Следует иметь ввиду того, что при обнаружении элементов устройства съема информации или канала утечки информации возможны два варианта дальнейших действий поисковой бригады.

В первом варианте - поисковая бригада, в зависимости от пожелания руководства объекта поиска, должна предпринять меры по блокировке, нейтрализации или уничтожения канала утечки информации, а обнаруженные элементы устройства съема информации или устройство в целом должно быть изъято.

Во втором варианте - устройство съема информации продолжает функционировать, а канал утечки информации используется руководством объекта поиска по своему усмотрению, не исключая возможности использования этого канала для формирования в нём дезинформации для прогнозируемого противника.

В плане поисковых исследований как при подготовке к ним, так и при проведении всех работ на объекте поиска центральное место должна занимать конспирация на всех этапах их проведения, начиная от легендирования появления поисковой бригады на объекте поиска и кончая обеспечения легендирования ухода бригады из объекта поиска.

Наряду с этим в плане поисковых исследований должна быть запланирована линия поведения каждого участника поисковой бригады и бригады в целом, в частности, должна быть указана конспиративность ведения разговоров на объекте поиска (обращение друг к другу в процессе проведения работ, взаимодействие между собой и с сотрудниками организации объекта поиска и т.д.).

План поисковых исследований разрабатывается опытными сотрудниками, которые, как правило, осуществляют первоначальное изучение объекта поиска и его окружения и которые в последующем может быть руководителем поисковой бригады

Для каждого намечаемого объекта поиска должен быть назначен руководитель поисковой бригады, в обязанность которого входят анализ исходной информации, разработка в устном или письменном виде плана проведения поисковых работ, подготовка к их проведению и организация работ на объекте поиска.

Руководитель поисковой бригады должен:

-установить контакт с руководителем или лицом ответственным за безопасность организации объекта поиска;

-разработать легенду своего появления на объекте поиска, которая в последующем по возможности должна вписываться в проведение поисковых исследований на всех этапах их осуществления;

-добыть сведения и материалы, необходимые как при изучении объекта поиска, так и в процессе проведения поисковых исследований;

-разработать план поисковых исследований;

-разработать и согласовать план конспирации и оперативного обеспечения поисковых работ;

-обеспечить конспиративную доставку и внос аппаратуры и материалов на объект поиска и вынос их с объекта поиска , а также их хранение;

-принимать участие в организации и проведении поисковых исследований;

-координировать действия всех сотрудников поисковой бригады.

Подготовка к поисковым исследованиям должна заканчиваться разработкой плана работ поисковых работ, с обязательным обеспечением необходимой документации. В состав документации могут входить:

-план прилегающей местности в радиусе до 500 метров с указанием, по возможности, принадлежности зданий и их назначения;

-поэтажные планы здания, в котором располагается объект поиска, с указанием смежных с обследуемыми помещениями;

-характеристика элементов строительных конструкций (стен, пола, потолочных перекрытий и т.д.) и материалов отделки;

-схемы разводки водо и теплопроводных коммуникаций;

-схемы проводных коммуникаций объекта поиска с указанием всех щитов, распределительных коробок и других элементов, которые в некоторых случаях территориально могут быть размещены вне, объекта поиска;

-планировка обследуемых помещений с указанием размещения предметов интерьера, мебели, оборудования, радио и телеаппаратуры средств связи, оргтехники и т. д.;

-сведения о лицах и времени нахождения их в смежных помещениях;

-перечень лиц, посвященных в характер поисковых работ;

-легенды проведения поисковых работ на всех этапах их осуществления;

-план мероприятий по прикрытию работ поисковой бригады в процессе их заезда, проведения поисковых работ и отъезда с объекта поиска;

-перечень поисковой аппаратуры;

-план действия на случай обнаружения устройств съема информации или каналов утечки информации;

-график выполнения работ с указанием

сроков, последовательности, исполнителей и ответственных как за всю работу, так и за определенные виды работ.

Полнота отражения документов диктуется практической необходимостью.

Для каждого конкретного объекта поиска вышеперечисленные документы могут уточняться и дополняться.

РАЗДЕЛ 4. ОСМОТР И ПРОВЕРКА ПРЕДМЕТОВ БЫТА И ИНТЕРЬЕРА, НАХОДЯЩИХСЯ НА ОБЪЕКТЕ ПОИСКА

Осмотр и проверка предметов быта и интерьера, находящихся на объекте поиска, с целью определения наличия (отсутствия) в их элементах устройств съема информации, должна начинаться с визуального фиксирования, а в некоторых случаях, и фотографирования мест расположения всех предметов в обследуемом пространстве.

Осмотр и проверка предметов быта и интерьера, а также все последующие работы поисковых исследований должны проводиться с учётом возможного наличия средств видеонаблюдения на объект" поиска. Перед началом поисковых исследований система видеонабдюдения должна быть на время проведения, по возможности, выключена полностью или частично в местах поисковых работ.

Кроме этого перед началом осмотра необходимо обратить внимание на возможные метки, которые могут оставляться с той или иной целью, в том числе и с целью фиксирования места размещения определённых предметов в которых могут быть внедрены устройства съема информации.

В качестве меток может быть использовано определённое расположение разных предметов, расположение на предметах в определённом порядке ниток, волосинок, пыли, следов пальцев и другие характерные пометки, а также метки наносимые специальным химическим составом, которые могут визуально или с помощью луп обнаружены.

Визуальный осмотр и проверку предметов быта и

интерьера объекта поиска целесообразно проводить от общего к частному.

Сначала визуальному осмотру подлежит вся территория объекта поиска, в том числе и, по возможности, территории не входящие в объект поиска, и осмотр которых, в некоторых случаях, может не предусмотрен планом. Для этого один из опытных сотрудников поисковой бригады тщательно осматривает все предметы, не прикасаясь к ним, обращая особое внимание на возможные изменения расположения их от ранее установленного порядка по различным признакам (смещены, повёрнуты, переставлены местами, друг относительно друга и т.д.), на неплотно прилегающий палас или линолеум к полу, ковров к стене, не приклеенные обои и на другие возможные признаки. Следует также обращать внимание на потемнение (посветление) в отдельных местах обоев, ковров, пола, свежеокрашенные стены, потолки, обшивку салона автомашины, срубленное дерево, согнутые кусты, помятую траву, на появившиеся временные сооружения (палатки, будки и т.д.), временные стоянки автомашин и другие характерные изменившиеся особенности мест и находящихся на них предметов.

После общего осмотра приступают к детальному визуальному осмотру конкретных мест и предметов, который должен проводиться с учётом выявленных ранее особенностей.

Визуальный осмотр предметов быта и интерьера осуществляется со всех сторон. Мебель должна быть отодвинута от стен и друг от друга, а ящики выдвинуты, содержимое ящиков переложено и тщательно осмотрено. Кроме этого необходимо пристально осмотреть все дверные ручки, запирающие устройства, вешалки, фирменные знаки и другие

предметы, обращая особое внимание на возможные подозрительные отверстия, инородные вставки, неестественно запачканные места и другие особенности предметов.

Подозрительные места и отверстия целесообразно осматривать с помощью луп с разными коэффициентами увеличения.

Осмотр труднодоступных мест на объекте поиска (межмебельные пространства вентиляционные каналы, места за батареями отопления, дымоходы и т.д.) необходимо осматривать с помощью досмотровых комплектов.

Одним из наиболее практически удобным и эффективным досмотровым комплектом является изделие "ШМЕЛЬ-2", в состав которого входит телескопическая штанга (длина 1550 мм), два смежных зеркала различного размера и конфигурации и фонарь подсветки.

Для окончательного выяснения наличия (отсутствия) в предметах быта и интерьера объекта поиска, выявленных в результате визуального осмотра целесообразно проводить углублённую их проверку с помощью металлоискателя и нелинейного локатора.

Металлоискатель обеспечивает фиксацию наличия в обследуемых предметах быта и интерьера и других местах объекта поиска металлических предметов, которые могут присутствовать в устройствах съема информации.

В качестве металлоискателя можно порекомендовать портативный вихре токовый металлоискатель типа "ВМ-12Н"или высокочувствительный точечный металлоискатель типа "ХМД-02", которые обеспечивают обнаружение

однокопеечной монеты на расстояние не менее 10 см и обнаружение металлической пластины с размерами 100х100х1 мм на расстоянии до 30 см. При использовании на объекте поиска металлоискателя следует убирать от обследуемого места металлические предметы на расстояние превышающее допустимое для выбранного металлоискателя.

Наиболее эффективным прибором, обеспечивающим быстрое и достоверное выявление и локализации мест возможного размещения элементов устройств съема информации (микрофонный усилитель, средства звукозаписи, подслушивающие устройства и т. д.), а также мест размещения радио взрывателей и других устройств, содержащих полупроводниковые элементы в предметах быта и интерьера объекта поиска является нелинейный локатор.

В нелинейном локаторе используется принцип приёма высокочастотного сигнала отражённого от предметов быта и интерьера и других предметов, в составе которых имеются полупроводниковые элементы, При этом следует отметить, что нелинейный локатор формирует сигнал наличия в том или ином месте размещения элементов устройств съема информации не зависимо от того включены или выключены они.

В настоящее время широкое применение находят нелинейные локаторы «Родник», "NR-900M", "NR-900E", "ОБЬ" и "ШЛЮЗ", параметры которых приведены в таблице 1.

Таблица 1

Параметры нелинейно-го локатора	Тип нелинейного локатора				
	Родник-2	NR-900 M	NR-900 E	Обь	Щлюз
Вид излучения	Непрер	Импульс		Непрер.	Импульс
Анализи-руемые гармоники	2,3	2	2,3	2,3	2
Частота излучения, МГц	910	900	900	1000	650
Чувствите-льность приемника, дБВт	-145	-110	-115	145	-120
Время непрерыв-ной работы, час	2	6	6	4	6
Масса, кг	11	7	8	5	10

Все вышеназванные нелинейные локаторы, потребительские характеристики которых указаны в таблице 1., обеспечивают возможность определения наличия в том или ином предмете или в элементе строительной конструкции устройства съема информации и определение его место нахождения на глубине, например, в стене, не менее 50 сантиметров.

Следует обратить внимание, что в процессе проверки предметов быта и интерьера, имеющих (скрепки, шурупы и другие металлические элементы)

нелинейный локатор может сформировать сигнал, аналогичный сигналу от устройства съема информации.

Для различения сигналов, формируемых от устройства съема информации съема информации, но имеются крепёжные элементы, нелинейный локатор будет формировать прерывистый звуковой сигнал, а при наличии в обследуемых предметах устройства съема информации будет формироваться постоянный звуковой сигнал.

Для окончательного определения наличия (отсутствия) в обследуемом предмете устройства съема информации необходимо еще раз тщательно осмотреть с помощью луп с различными коэффициентами увеличения этот предмет или обследуемое место в элементе строительной конструкции, обращая внимание на возможное наличие в них отверстия, указывающего на наличие акустического канала утечки информации. После этого обследуемый предмет или обследуемое место проверить ещё раз металлоискателем и нелинейным локатором при различном расположении его относительно используемых приборов. Если снова металлоискатель и нелинейный локатор будет формировать прерывистый звуковой сигнал, указывающий на отсутствие в нем устройства съема информации, необходимо по возможности разобрать обследуемый предмет и убедиться о наличии (отсутствии) в нём устройства съема информации. Следует обратить внимание, что после разборки подозрительного предмета быта и интерьера и последующей визуальной оценки наличия (отсутствия) в них устройства съема информации необходимо их собрать и проверить функционирование в рабочем режиме.

Эффективность использования в поисковых

исследованиях металлоискателя и нелинейного локатора зависит от скорости перемещения их относительно обследуемого предмета (поверхности), которая не должна превышать 30 см/сек. в разных направлениях, и от удаления металлоискателя и антенны нелинейного локатора от обследуемого предмета (поверхности), величина которой не должна превышать 15 см.

При установке факта наличия в обследуемом предмете устройства съема информации необходимо оценить вид канала утечки информации и по возможности определить потребительские параметры (дальность передачи сигналов информации, ресурс работы, источник питания и т.д.) обнаруженного устройства съема информации. Вышеназванные параметры обнаруженного устройства съема информации могут быть определены на объекте поиска.

В дальнейшем руководитель поисковой бригады совместно с руководством организации объекта поиска решает вопрос о дальнейшем судьбе устройства съема информации, которая может реализована по следующим направлениям:

-устройство съема информации изымается;

-устройство съема информации консервируется;

-устройство съема информации используется для дезинформации вероятного противника.

При принятии решения вопроса по изъятию из мест негласно установленного устройства съема информации поисковая бригада осуществляет его изъятие и демонтаж таким образом, чтобы устройство осталось работоспособным, а место его размещения, по возможности, не отличалось от первоначального вида.

После изъятия устройства съема информации

производится измерение в лабораторных условиях его электрических характеристик, на основании которых уточняются следующие потребительские параметры найденного устройства съема информации:

- канал утечки информации (акустический, радийный, телефонный, радиотелефонный, электросетевой и т.д.);
- метод внедрения устройства съема информации (заходный или беззаходный);
- вид несанкционированно снимаемой информации (акустические сигналы, сигналы телефонных переговоров, паразитные излучения компьютеров и т.д.);
- способ несанкционированного съема сигналов информации (индуктивный, низкочастотный, высокочастотный, дистанционный и т.д.);
- вид источника питания (автономный, электросеть 220 В);
- ресурс работы от автономного источника питания;
- ориентировочная дальность передачи сигналов информации (в пределах обследуемых помещений, до телефонного шкафа, до электросчетчика, в пределах нескольких помещений и т.д.);
- ориентировочное время внедрения устройства съема информации;
- технический и технологический уровень изготовления изделия.

Оценку по всем вышеперечисленным потребительским параметрам могут произвести специалисты, имеющие большой опыт поисковых исследований и работы с радиотехническими средствами.

При принятии решения о консервации найденного устройства съема информации последующие работы могут проводиться по двум возможным вариантам:

-по первому варианту устройство съема информации дорабатывается таким образом, чтобы оно оставалось работоспособным, но съем и передача сигналов информации не осуществлялась. Для устройства съема информации, использующего в качестве канала передачи сигналов информации акустический канал это может быть достигнуто: во-первых, путём заклеивания акустического отверстия липкой лентой, пластилином или другим материалом; во-вторых, путём разрыва связи устройства с каналом передачи сигналов. Для других обнаруженных устройств съема информации они дорабатываются таким образом, в результате чего по используемому им каналу утечки информации сигналы не передаются.

-по второму варианту "консервируется" не устройство съема информации, а объект поиска, путём отсутствия в нём сигналы конфиденциальной информации т.е. в этих местах не производятся разговоры, переговоры и компьютерные расчеты, несущие конфиденциальную информацию. Следовательно в этом случае по возможным каналам утечки информации передаются сигналы не несущие никакой конфиденциальной информации..

При принятии руководством организации объекта поиска решения по использованию найденного устройства съема информации для дезинформации прогнозируемого противника поисковая бригада должна уточнить следующие его потребительские характеристики:

-используемый канал утечки информации;

-способ съема сигналов информации;

-вид источника питания устройства съема информации (автономный, электросетевой или телефонный);

-ресурс работы системы съема и передачи сигналов информации при автономном питании;

-дальность передачи сигналов информации.

После этого необходимо проверить функционирование системы съема информации.

Следует отметить, что для подтверждения передачи дезинформационных сведений прогнозируемому противнику необходимо: во-первых создать тракт передачи-приёма сигналов информации, используя в качестве передатчика найденное устройство съема информации, а в качестве приёмника сигналов информации целесообразно использовать приёмник с параметрами, аналогичными приёмнику, используемому прогнозируемым противником; во вторых, помочь руководству объекта поиска в разработке сценария дезинформационной среды, который должен иметь обратную связь с предпринимаемыми действиями прогнозируемого противника.

Такой алгоритм функционирования системы и сценария её использования позволит подтвердить или опровергнуть прогнозируемого противника и выяснить его замыслы.

После окончания дезинформационной игры по решению руководства объекта поиска устройство съема информации может быть измято или законсервировано.

Процедура изъятия или консервации выполняется таким же образом, как и ранее описана.

Следует отметить, что независимо от потребительских параметров найденного устройства

съема информации после дезинформационной игры его желательно оставить вне рабочем состоянии.

После окончании всех работ изъятое устройство съема информации по желанию руководства организации объекта поиска может передано поисковой бригаде или оставлено в организации.

В случае передачи найденного подслушивающего устройства поисковой бригаде она, если имеется такая возможность, собирает весь тракт съема и передачи сигналов информации, измеряет и уточняет его основные потребительские характеристики (метод внедрения, способ съема сигналов информации, рабочий диапазон частот, дальность передачи сигналов информации, напряжение питания, время непрерывной работы, ориентировочное время внедрения и т. д.), на основании чего составляется акт обнаружения устройства съема информации, содержание которого целесообразно согласовать с руководством объекта поисковых исследований. Акт поисковых исследований может быть составлен в произвольной форме. Один из возможных вариантов акта поисковых исследований приведён в приложении 2.

По окончании осмотра и проверки предметов быта и интерьера на наличие в них устройств съема информации они должны быть установлены на прежнее зафиксированное в начале работы место.

РАЗДЕЛ 5. ПОИСК УСТРОЙСТВ НЕСАНКЦОНИРОВАННОГО СЪЁМА ИНФОРМАЦИИ, ВНЕДРЁННЫХ В ЭЛЕКТРОННЫЕ ПРИБОРЫ

Поиск устройств негласного съема информации в электронных приборах (телефонных аппаратах, телевизорах, ксероксах, радиоприёмниках, компьютерах и т.д.) на объектах поиска целесообразно осуществлять в следующей последовательности:

Сначала, как и было описано ранее, проводится зрительная или аппаратурная фиксация мест размещения всех электронных приборов объекта поиска.

Затем проводится анализ электромагнитного поля обследуемых электронных приборов как в работающем, так и в не работающем состояниях, позволяющий выявить и локализовать место размещения радиоподслушивающих устройств съема информации.

С целью оперативного обнаружения радиоподслушивающих устройств в электронных приборах по электромагнитному полю целесообразно использовать индикаторы поля, позволяющие не только обнаружить, но и локализовать место их размещения не зависимо от используемого вида модуляции, диапазона частот и излучаемой мощности.

Примечание. Для локализации мест размещения устройств съема информации и идентификации акустических сигналов объекта поиска целесообразно использовать бытовой радиоприёмник. С этой целью на всё время проведения поисковых работ радиоприёмник должен находиться во включённом состоянии, ибо акустический сигнал радиоприёмника кроме идентификации акустических сигналов

объекта поиска должен выполнять функцию акустической маскировки проводимых поисковых работ.

Принцип действия индикаторов поля основан на широкополосном детектировании электрического (электромагнитного) поля и формирования сигнала тревоги при приближении его антенны к электронному прибору, в котором размещается работающее радиоподслушивающее устройство.

Радиус обнаружения радиоподслушивающего устройства зависит от излучаемой мощности и для всех известных индикаторов поля, в том числе и индикаторов поля, потребительские параметры которых указаны в таблице 2, не превышает одного метра при мощности излучения радиоподслушивающего устройства более 5 мВт.

Таблица 2

Параметры индикатора поля	Наименование индикатора поля			
	Д-008	Рич-2	ИПФ-6	Шкатулка
Диапазон частот, МГц	50-1500	50-1300	30-2500	50-1500
Чувствительность на частотах, мВ				
110МГц	2	2	1	1,5
800 МГц	6	1	1	1,5
1500 МГц	6	1	1	1,15
Динамич. диапазон, дБ	20	35	30	30

Как видно из таблицы наиболее часто встречаемые индикаторы поля имеют примерно одинаковые потребительские параметры.

Следует отметить, что все индикаторы поля, потребительские параметры которых приведены в таблице 2, имеют акустическую обратную связь, проявляющуюся в виде акустической завязки. Акустическая завязка сводит к минимуму возможных ложных срабатываний и позволяет идентифицировать радиоподслушивающие устройства по тональному звуковому сигналу, уровень которого увеличивается при приближении к работающему радиоподслушивающему устройству.

Наряду с этим ряд индикаторов поля выполняют не только функции обнаружения и локализацию мест размещения радио подслушивающих устройств, но и ряд других функций. Так, например, индикатор поля Д-008 обеспечивает поиск устройств съема информации, внедрённых в различные проводные коммуникации, а индикатор поля РИЧ-2 - осуществляет измерение частоты, уровня источников радио-излучений и формирует сигнал тревоги при превышении измеренного электромагнитного поля фонового уровня на 10-15 дБ. Сформированный сигнал тревоги может передаваться на пункт охраны по проводным коммуникациям или по проложенным проводным линиям.

Во всех известных индикаторах поля имеется аттенюатор, обеспечивающий ослабление или усиление входного электромагнитного сигнала, что позволяет упростить процесс поиска места размещения радио или радиотелефонных подслушивающих устройств в условиях сложной электромагнитной обстановки порой имеющей

место на объекте поиска.

Как было сказано ранее поиск радио и радиотелефонных подслушивающих устройств в электронных приборах осуществляется как в включённом, так и выключенном состояниях.

Следует иметь ввиду, что для обеспечения надёжного поиска радио и радиотелефонных подслушивающих устройств в электронных приборах с использованием индикатора поля необходимо чтобы исследуемый электронный прибор был размещён таким образом, чтобы он находился от других приборов на расстоянии более одного метра. Такое размещение исследуемого электронного прибора исключит влияние на процесс обнаружения радиопередающих устройств, имеющихся в других приборах.

Перед началом поиска необходимо, по возможности, все электронные приборы выключить, выдвинуть антенну индикатора поля на два колена и включить его. После этого медленно перемещая антенну во всех возможных направлениях вдоль анализируемого электронного прибора производится обследование всех электронных приборов, находящихся на объекте поиска.

Если при приближении антенны индикатора поля к исследуемому электронному прибору он формирует сигнал тревоги в виде акустического сигнала характерного для объекта поиска и изменяющегося при резких хлопках и стуках, а уровень его увеличивается при приближении индикатора поля к испытываемому электронному прибору и наоборот уменьшается при удалении, это указывает на то, что в нём возможно размещено радиоподслушивающее устройство. При этом если сигнал обусловлен работой акустического радио

подслушивающего устройства, то на выходе индикатора поля будут прослушиваться признаки акустического сигнала объекта поиска, а при наличии в электронном приборе работающего радиотелефонного подслушивающего устройства будут прослушиваться признаки телефонных переговоров.

Следует обратить внимание, что при большом уровне акустического сигнала в головных телефонах индикатора поля его можно уменьшить или потенциометром индикатора поля или путём уменьшения длины его телескопической антенны.

В процессе анализа электронных приборов индикатор поля может сформировать ложный сигнал, который обусловлен наличием электромагнитного поля от вещательной или телевизионной станции.

Отличительной особенностью этого ложного акустического сигнала, обусловленного работой вещательной или телевизионной станцией, является наличие в нём признаков музыкальной или речевой передачи не характерных для объекта поиска, либо признаков характерного "рокота", обусловленного детектированием строчной развёртки телевизионного сигнала.

Такой алгоритм поиска устройств съема информации в электронных приборах с использованием индикатора поля необходимо осуществить при включённом и выключенном состояниях каждого анализируемого электронного прибора, а остальные электронные приборы при этом всегда должны находиться в выключенном состоянии.

Если подтверждается, что источником электромагнитного излучения является исследуемый электронный прибор, переходят к визуальному

осмотру и по возможности к его разборке. Визуальный осмотр и разборку электронного прибора осуществляют по методике, изложенной ранее. Для этих целей поисковая бригада должна иметь различные инструменты, лупы с различными коэффициентами увеличения, приборы и приспособления, полный набор которого должен имеет:

- Обнаружитель радиоподслушивающих устройств;
- Обнаружитель электроакустических подслушивающих устройств;
- Имитатор передатчика электросетевых подслушивающих устройств;
- Комплекс средств для обнаружения сигналов подслушивающих
  устройств в проводных коммуникациях;
- Телефонный усилитель;
- Складное портативное досмотровое зеркало с подсветкой типа изделия "ШМЕЛЬ";
- Металлодетектор;
- Лупы;
- Паяльник;
- Мультитестер;
- Бытовой радиоприёмник;
- Головные телефоны;
- Фонарь узконаправленный;
- Две отвёртки (простая и крестовая);
- Плоскогубцы;
- Дрель;
- Пинцет;
- Элемент питания;
- Канифоль, припой;
- Соединительные провода;
- Практическое руководство по поиску

устройств съема информации.

Аппаратура, входящая в комплект "ШТУРМ", питается от автономного источника тока или от электросети переменного тока 220В.

Вся вышеперечисленная аппаратура, инструмент и приборы желательно чтобы они размещались в атташе-кейсе.

Такой набор аппаратуры, инструментов и приспособлений желательно, чтобы он питался от автономного источника тока или, в крайнем случае от сети 220В

Анализируемый электронный прибор вскрывают и тщательно визуально и с помощью луп осматривают все радиоэлементы и печатные платы. Обращая внимание на возможное наличие в них дополнительных плат или радиоэлементов, изменения в штатных печатных платах, просматривая номиналы и размеры радиоэлементов и наличия в них отличительных признаков. Причём особое внимание должно быть уделено конденсаторам ёмкостью свыше 20мкФ. поскольку в них могут быть размещены радиоэлементы радио, радиотелефонных или телефонных подслушивающих устройств.

Отличительным признаком таких конденсаторов является наличие у них, как правило, со стороны выводов акустического отверстия диаметром около 1 мм.

Если в процессе визуального осмотра не найдены радиоэлементы подслушивающих устройств далее осуществляют их поиск по характерным признакам, которые, как правило, обладают монтаж изделия.

Необходимо иметь ввиду, что если монтаж электронного прибора выполнен в заводских

условиях пайки, как правило, имеют одинаковую площадь и высоту и практически не имеют заусенцев, а печатные платы покрыты светлым лаком и на их поверхностях отсутствует канифоль. Это подтверждается тем, что в местах пайки радиоэлементов подслушивающих устройств, если такие имеются, будет просматриваться желтизна.

Для проверки наличия в пайках заусенцев необходимо провести ладонью по печатной плате. В тех местах, где были осуществлены дополнительные пайки, будут ощущаться острые заусенцы.

Для окончательного убеждения наличия (отсутствия) в исследуемом приборе радиоэлементов подслушивающих устройств необходимо произвести сравнение их расположения с расположением радиодеталей на монтажной схемой (если такая имеется), копией платы или с фотографией расположения радиоэлементов на плате аналогичного изделия. Эту работу, как правило, могут проводить профессиональные поисковые бригады, в которых имеется набор электрических и монтажных схем различных электронных приборов.

Если отличительных признаков по монтажным платам нет, необходимо повторить оценку наличия электромагнитного излучения в разобранном исследуемом электронном приборе по вышеописанной методике при включенном и выключенном его состояниях.

При повторном подтверждении наличия электромагнитного излучения, которое может принадлежать подслушивающему устройству, анализируемый электронный прибор ещё раз разбирают и тщательно проводят визуальный осмотр и приборный и приборный анализ и окончательно

убеждаются в наличии (отсутствии) подслушивающих устройств.

При обнаружении в анализируемом электронном приборе подслушивающего устройства необходимо, по возможности восстановить его функционирование в разобранном электронном приборе, после чего необходимо сообщить руководителю организации объекта поиска об найденном устройстве и доказательно показать ему наличие его, в том числе, если это возможно, и показать его функционирование. Затем совместно с руководителем объекта поиска решить вопрос по изъятию (не изъятию) подслушивающего устройства из анализируемого электронного прибора.

При согласии руководителя объекта поиска на изъятие подслушивающего устройства или его элементов из анализируемого электронного прибора все радиоэлементы, относящиеся к нему, в определённой последовательности выпаиваются, электронный прибор собирается и после проверяется его функционирование. Причём, если анализируемый электронный прибор не функционирует, необходимо в определённой последовательности подпаивать ранее отпаянные радиоэлементы, которые по нашему предположению относились к подслушивающему устройству, и добиться его функционирования.

Как было описано ранее по согласованию с руководством объекта поиска радиоэлементы подслушивающего устройства или устройство в целом может быть оставлено организации или передано поисковой бригаде для оценки его потребительских параметров.

Поисковая бригада, если имеется такая возможность, в лабораторных условиях собирает весь

тракт съема и передачи сигналов информации, состоящий из найденного подслушивающего устройства и приёмного устройства, измеряет и уточняет его основные потребительские параметры (вид подслушивающего устройства, метод внедрения, способ съема сигналов информации, рабочий диапазон частот, дальность передачи сигналов информации, напряжение питания, время непрерывной работы, ориентировочное время внедрения и т.д.), на основании чего составляется акт поисковых исследований и обнаружения подслушивающего устройства, содержание которого целесообразно согласовать с руководством объекта поиска.

Акт может быть составлен в произвольной форме. Образец акта поисковых исследований приведен в приложении 2.

РАЗДЕЛ 6. ИССЛЕДОВАНИЕ ЭЛЕКТРОМАГНИТНОЙ ОБСТАНОВКИ В ПОМЕЩЕНИЯХ, В АВТОМАШИНАХ И НА ОТКРЫТОЙ МЕСТНОСТИ

Исследование электромагнитной обстановки на объектах поиска в помещениях (в офисах, в банках, на складах, в торговых залах и т.д.), в автомашинах (в салоне, вне сагана автомобиля и т.д.) и на открытой местности (в сквере, на опушке леса, на пляже и т.д.) проводится с целью обнаружения и локализации электромагнитных излучений в широком диапазоне частот, образующихся; во первых, за счёт побочных паразитных электромагнитных излучений, которые могут создавать электронные приборы, находящиеся в рабочем или в нерабочем состояниях (звукоусилительные установки, магнитофоны, ЭВМ различного назначения, отечественные и импортные телефонные аппараты, переговорные устройства, аппаратура диспетчерской связи и т.д.); во вторых, за счёт радио излучений подслушивающих устройств, внедрённые в обследуемые объекты поиска и в сопредельных с ним объектах.

Таким образом знание электромагнитной обстановки позволит установить на объекте поиска наличие возможного электромагнитного канала утечки информации и возможное наличие в нём радио или радиотелефонных подслушивающих устройств.

Исследование электромагнитной обстановки необходимо начинать с детального конспиративного визуального осмотра всех мест объекта поиска, описание которого произведено ранее, а также визуального и аппаратурного осмотра сопредельных помещений, зданий и других мест с целью определения возможных вариантов дистанционного

съема информации с использованием лазерных устройств и радио облучающих систем.

После визуального осмотра определяют возможное размещение стационарных или мобильных пунктов приёма побочных электромагнитных излучений электронных приборов объектов поиска и сопредельных с ним объектов, а также определяют размещение возможных пунктов приёма сигналов подслушивающих устройств, внедрённых в обследуемый объект поиска или в сопредельных с ним местах.

При визуальном осмотре особое внимание необходимо обратить на окна сопредельных помещений, на стоящие на улице автомобили и на временные постройки (палатки, будки и т.д.) и находящихся в них или рядом с ними людей и предметов.

Следует также обратить внимание, что с целью повышения надёжности выявления пунктов приёма необходимо применять меры активизации их функционирования. Для активизации работы пунктов приёма сигналов информации необходимо сформировать дезинформацию типа проведения лжеинформационных совещаний, осуществления перестройки работы организации объекта поиска и смежных с ней организаций, смены кабинетов руководителей и т. д. При этом в процессе осуществления дезинформационной работы необходимо пристально наблюдать за действием людей возле предполагаемого пункта приёма. Длительность проведения дезинформационной работы определяется многообразием возможных пунктов приёма сигналов информации и необходимостью строгого соблюдения конспирации их осуществления. Поэтому дезинформационная работа может продолжаться от нескольких минут до

нескольких суток.

Для проведения работы по выявлению возможного пункта приёма и обработки негласно снимаемых сигналов информации необходимо использовать моникулятор панкратического типа "МП", обеспечивающий ведение наблюдения за местностью и различными объектами, удалёнными на расстояние до 600 метров от объекта наблюдения.

Кроме этого для наблюдения объектов в условиях слабого освещения или в полной темноте целесообразно использовать приборы ночного видения "МЕДИТОН-302", "МЕДИТОН-312" и "ТИТАН-720", позволяющие осуществить наблюдения в вечернее и ночное время суток.

Принцип действия приборов ночного видения основан на использовании в них электронно-оптических преобразователей, которые усиливают свет, отраженный от наблюдаемого объекта.

Основные параметры вышеназванных приборов ночного видения, практически, одинаковы. Однако следует отметить, что применение в приборе ночного видения "ТИТАН-720" активно-импульсного (локаторного) режима позволяет вести наблюдение в условиях дождя, тумана, дыма, а также позволяет видеть объекты сквозь легкую листву деревьев и производить измерение расстояния до объекта с точностью до 2% от измеряемой величины.

Использование приборов ночного видения "МЕДИТОН-302" и "МЕДИТОН-312" совместно с фотоаппаратом и видеокамерой позволяет фотографировать или производить видеозапись на расстоянии до 250 метров.

Наряду с вышеописанными приборами ночного видения для оперативного применения в условиях объекта поиска могут быть рекомендованы очки ночного видения "Д-2М", "Д-2МВ", "Д-202", позволяющие

наблюдать объекты в условиях слабого освещения или в полной темноте. Очки ночного видения устанавливаются на шлем маске, которая закрепляется на голове.

Очки ночного видения могут использоваться как бинокль, для этого они должны быть укомплектованы сменными длиннофокусными объективами, обеспечивающими большое увеличение и повышенную дальность видения.

Изучение обстановки вокруг объекта поиска заканчивается подтверждением или не подтверждением версии наличия пунктов приёма сигналов информации.

По окончании изучения сопредельной территории, помещений, автомашин и зданий и определение наличия или отсутствия в них пунктов приёма сигналов информации корректируется, если это необходимо, план работы поисковых исследований в целом и в частности план измерения электромагнитной обстановки на объекте поиска.

В настоящее время для измерения электромагнитной обстановки на объектах поиска имеется большой выбор программно-аппаратных комплексов.

Основу программно-аппаратных комплексов составляет сканирующий радиоприёмник, функционально сопряжённый с ПЭВМ и работающий под управлением специальной программы SEDIF PLUS, SEDIF PRO или RADIO SEARCH.

Наиболее распространенным техническим средством, обеспечивающим просмотр загрузки радиодиапазона во времени, расчет амплитудного спектра анализируемого радиодиапазона, определение уровня шума, обнаружение сигналов узкополосных радиосигналов и т. д, является

программно-аппаратный комплекс быстрого панорамного анализа радиочастотного спектра "АРК-ПА2".

Программно-аппаратный комплекс "АРК-ПА2", а также другие технические средства аналогичного назначения, в состав которых входит компьютер, сканирующий приёмник "AR-3000 A", работающий под управлением специальной программы SEDIF имеют следующие основные потребительские параметры:

- диапазон рабочих частот 25-2000 МГц;
- ширина суммарного диапазона частот панорамного анализа:
  минимальная- 3МГц,
  максимальная- 30 МГц;
- динамический диапазон уровней входных сигналов не менее - 50дБ;
- чувствительность по входному немодулированному радиосигналу не хуже 1 мкВ.

Программно-аппаратный комплекс с подобными параметрами позволяет составить карту занятости радио эфира на объекте поиска, выделить и исключить из дальнейшего рассмотрения известные радиоизлучения (легальные и часто встречающиеся), а также выявить спектральные составляющие электромагнитного поля, относящиеся к тем или иным радиоподослушивающим устройствам, имеющим место на объекте поиска.

Для выявления радио излучений на объекте поиска, относящихся к радиоподслушивающим устройствам, поисковая бригада должна иметь базу данных занятости радио эфира того района в котором оценивается электромагнитная обстановка. Имеющаяся база данных занятости радио эфира

должна заноситься в компьютер при каждом измерении электромагнитной обстановки и учитываться в процессе будущих поисковых исследований.

Имеющаяся база данных занятости радио эфира и программно-аппаратный комплекс позволяют профессиональной поисковой бригаде измерить электромагнитную обстановку, на основании которой оцениваются возможные каналы утечки информации и определяется наличие (отсутствие) на объекте поиска подслушивающих устройств.

Измерение электромагнитной обстановки на объекте поиска производится в каждом помещении, в салоне автомобиля (при включённом и выключенном двигателе) и на открытой местности.

При площадях объекта поиска менее 100х2м программно-аппаратный комплекс должен размещаться по возможности в центре объекта поиска. При площадях объекта поиска более 100х2м программно-аппаратный комплекс размещается в двух и более местах, удаленных друг от друга на расстоянии не более 10 метров.

В каждом месте размещения программно-аппаратного комплекса измерение электромагнитной обстановки в анализируемом диапазоне частот с различными видами модуляции производится трехкратным повторением.

После измерения электромагнитной обстановки в выбранных местах на объекте поиска с помощью компьютера составляется карта занятости радио эфира и производится выделение и исключение из неё известных спектральных составляющих электромагнитного поля.

Затем осуществляется сравнение оставшихся

спектральных составляющих электромагнитного поля с имеющимся в памяти данных компьютера, полученных в процессе ранее проведенных поисковых исследований и исключение их из полученных в результате измерения.

Оставшиеся спектральные составляющие электромагнитного поля являются подозрительными. С помощью программно-аппаратного комплекса еще раз производят измерение электромагнитного поля при различном расположении его и различных режимах функционирования электронных приборов, имеющих место на объекте поиска.

Если при повторном измерении электромагнитного обстановки во всех местах объекта поиска уровень каких-либо подозрительных спектральных составляющих электромагнитного поля изменился незначительно (не более нескольких процентов), тогда в сканирующем приёмнике программно-аппаратного комплекса необходимо изменить вид модуляции и полосу обзора и с помощью головных телефонов попытаться прослушать акустические сигналы. Если акустические сигналы объекта поиска не прослушиваются, следовательно, подозрительные сигналы в этих местах не относятся к радиоподслушивающим устройствам.

Если при повторном измерении электромагнитного поля уровень подозрительных спектральных составляющих изменился существенно и все излучающие электронные приборы выключены, следовательно, источник радиосигнала находится в ближней зоне (внутри объекта поиска) и для его локализации необходимо использовать индикатор поля.

Определение места внедрения радиоподслушивающих устройств с использованием индикатора

поля осуществляется аналогичным образом, что и ранее описано.

Если при повторном измерении электромагнитного поля и при включении того или иного электронного прибора уровень подозрительных спектральных составляющих изменяется, это указывает на то, что этот электронный прибор формирует электромагнитные излучения, которые могут быть источником утечки конфиденциальной информации.

Если в процессе поисковых исследований в обследованном месте не были обнаружены подозрительные источники электромагнитных излучений программно-аппаратный комплекс переносят в следующее место и процесс измерения электромагнитной обстановки повторяется

При обнаружении в том или ином месте объекта поиска устройства съема информации в дальнейшем поисковая бригада осуществляет работу по изъятию и определению потребительских параметров элементов и устройств в целом и совместно с руководителем объекта поиска рассматривает вопрос использование его.

РАЗДЕЛ 7. ПОИСК УСТРОЙСТВ СЬЁМА ИНФОРМАЦИИ В ПРОВОДНЫХ КОММУНИКАЦИЯХ

Анализ материалов, полученных Акционерным обществом «ЩИТ» при проведении поисковых исследований на различных объектах поиска показывает, что для негласного съема и передачи конфиденциальной информации используются различные проводные системы связи и различные проводные коммуникации.

Чаще всего для этих целей используются абонентская телефонная сеть, офисная телефонная сеть, электрическая сеть и радиотрансляционная сеть.

Практика проведения поисковых исследований показывает, что наиболее целесообразно проводить проверку проводных систем связи и проводных коммуникаций на наличие в них устройств съема информации в следующей последовательности:

- проверка электрической сети;
- проверка абонентской и офисной телефонной сети;
- проверка радиотрансляционной сети.

Для проведения поиска устройств съема информации, использующих различные возможные каналы утечки информации, в том числе и проводные коммуникации, могут быть применены различные приборы, инструменты и приспособления. Акционерное общество «ЩИТ» для этих целей выпускает комплект аппаратуры, инструментов и приспособлений "ШТУРМ", обеспечивающий комплексную проверку всех возможных проводных каналов утечки информации и изъятие из них найденных устройств съема информации. Описание комплекта "ШТУРМ" произведено в пятом разделе настоящего учебного пособия.

Поиск устройств съема информации во всех проводных систем связи и проводных коммуникациях, в том числе и в электрической сети, целесообразно начинать с обследования коммутационных и электроустановочных элементах.

Перед обследованием коммутационных и электроустановочных элементов электросети необходимо, если такая возможность имеется, обесточить всю обследуемую электросеть и с помощью мультитестера убедиться в отсутствии напряжения во всех электрических розетках объекта поиска.

Если по производственной или по другой причине отключение напряжения электросети на объекте поиска не представляется возможным, обследование коммутационных и электроустановочных элементов и всей электросети в целом должны проводить не менее двух высококвалифицированных сотрудников поисковой бригады, имеющих право работы электромонтёрами с напряжением до 380 В.

В начале обследования электросети сотрудники поисковой бригады, используя инструменты и приспособления комплекта "ШТУРМ", поочерёдно снимают крышки со всех розеток, выключателей и других элсктроустановочных и коммутационных элементов.

Затем визуально с помощью луп с коэффициентам усиления не мене 20 осматривают все детали обследуемых блоков, обращая особое внимание на места установки этих элементов, поскольку чаще всего устройства съема информации и их элементы устанавливаются в обследуемых местах или иод выключателем, под розеткой и в другие места внутри них или под ними.

После осмотра коммутационных и установочных блоков целесообразно снять плафоны, люстры и другие узлы осветительных приборов и визуально их осмотреть.

Настольные лампы и электросетевые удлинители следует разобрать и визуально убедиться, что внутри этих блоков отсутствуют или присутствуют устройства съема информации или их элементы.

Визуальный осмотр электросети заканчивается осмотром силового электрощитка, для чего необходимо снять лицевую крышку электрощитка и визуально осмотреть как крышку, так и внутри щитка, обращая внимание на подводящие электрические провода, которые по возможности, необходимо максимально вытянуть их из труб, ибо трубы, в которых размещаются провода являются удобным местом для размещения устройства съема информации или их элементов. На заключительном этапе проверки электросети на наличие в ней устройства съема информации необходимо подать напряжение питания по всем фазам, если оно было отключено, и проверить наличие напряжения в линии электросети.

Затем, с помощью комплекса "ШТРАФ" или аналогичной аппаратуры, определить фазы электросети во всех розетках.

Комплекс "ШТРАФ", как показано ранее, состоит из широкополосного детектора электрических сигналов (изделие "ШТРАФ-прм") и передатчика тонального сигнала (изделие "ШТРАФ-прд"). С этой целью в одну розетку вставляют изделие ("ШТРАФ-прд"), а во все другие розетки поочерёдно вставляют изделие ("ШТРАФ-прм"). При совпадении фаз электросети в розетке, в которую вставлено изделие "ШТРАФ-прд" и другой розетке, в которой вставлено изделие "ШТРАФ-прм" на

последней загорается левая лампочка.

После установления фаз электросети приступают к определению наличия (отсутствия) и локализации в ней устройств съема информации. Для этого можно использовать комплекс "ШТРАФ" или аппаратуру "ШПАГАТ", "ПИРАНЬЯ" или другую аппаратуру аналогичного назначения.

Основные потребительские параметры изделий "ШТРАФ", "ШПАГАТ" и "ПИРАНЬЯ" приведены в таблице 3.

Таблица 3

Параметры изделия	Наименование изделия		
	Штраф	Шпагат	Пиранья
Сигнал индикации	Световая	Световая, звуковая	Световая, звуковая
Диапазон частот, МГц	0,3-5000	0,3-5000	0,01-1000
Чувствительность, мВ	10	3	0,5
Полоса пропускания, кГц	3	5	10
Модуляция анализируемых сигналов	АМ, ЧМ	АМ, ЧМ	АМ,ЧМ
Напряжение питания, В	Эл/сеть 220В	Эл/сеть 220В	Эл/сеть 220В

Примечание. В таблице 3 для изделия "ПИРАНЬЯ" приведены основные потребительские параметры, относящиеся к его работе в режиме сканирующего анализатора проводных линий.

При применении комплекса "ШТРАФ" для определения наличия в электросети устройств съема информации необходимо в каждую розетку поочерёдно вставить изделие "ШТРАФ-прм" и при наличии в какой либо розетке сигналов в диапазоне частот свыше 30 кГц на изделии загорается левая лампочка. Это указывает на наличие в этой фазе электросети устройства съема информации.

Следует отметить, что изделие "ШТРАФ-прм" лишь фиксирует факт наличия в электросети сигналов устройств съема информации и не позволяет их идентифицировать, которое может быть осуществлено путём прослушивания акустических сигналов.

Аналогично применяется при обследовании электросети аппаратура "ШПАГАТ" и "ПИРАНЬЯ", исключением является то, что при обнаружении устройства съема информации они позволяют не только зафиксировать его наличие, но и прослушать акустические сигналы обследуемого помещения объекта поиска или помещений сопредельных с ним.

По характеру прослушиваемых акустических сигналов с помощью бытового радиоприёмника определяют помещение, в котором внедрено в элементы электросети устройство съема информации, а по уровню высокочастотного сигнала (уровню детектированного сигнала) определяют место его внедрения.

Следует отметить, что для передачи негласно снятых акустических сигналов объекта поиска на большие расстояния может использоваться радиоэлектросетевой ретранслятор. Наиболее вероятным местом размещения радиоэлектросетевого ретранслятора является электросетевой шкаф.

Поиск радиоэлектросетевого ретранслятора осуществляется аналогичным образом, как ранее

описано в разделе 6 "Исследование электромагнитной обстановки в помещениях, в автомашинах на открытой местности". Исключение составляет лишь то, что для локализации мест размещения устройств съема информации антенну индикатора поля необходимо перемещать вдоль линии электросети, останавливаясь на электроустановочных и коммутационных элементах (розетках, выключатели, счётчиках, лампах, удлинителях и т.д.)

При обнаружении на объекте поиска любых электросетевых устройств съема информации поисковая бригада показывает Руководству объекта поиска место внедрения и подключения устройства к элементам электросети и дают им возможность убедиться в наличии съема акустических сигналов путём их прослушивания с помощью головных телефонов, используя устройства "ШПАГАТ" или "ПИРАНЬЯ". Дальнейшая работа поисковой бригады с найденным устройством съема информации должна проводиться аналогичным образом, как ранее описано во втором разделе настоящего учебного пособия.

По окончанию проверки на объекте поиска электросети, не зависимо от того найдено ли было устройство съема информации или нет, приступают к проверке абонентской и офисной телефонной сетей.

Проверку абонентской и офисной телефонной сетей на наличие в них устройств съема информации проводят аналогичным образом, что и при обследовании электросети с учётом их особенностей и необходимости подключения устройств "ШПАГАТ" или "ПИРАНЬЯ" к телефонной линии.

Одной важнейшей особенностью телефонной сети является то, что по телефонной линии передаются сигналы телефонных переговоров и служебные сигналы.

Другой особенностью телефонной сети является то, что по телефонной линии могут передаваться сигналы телефонных переговоров и служебные сигналы не только в низкочастотном диапазоне частот, т.е. в диапазоне частот 300-3400Гц, но ив высокочастотном диапазоне частот. Например, при наличии на объекте поиска абонентской высокочастотной установки (АВУ) сигналы телефонных переговоров передаются в направлении "абонент-станция" в диапазоне частот 24,6-31,4 кГц, а в направлении "станция-абонент "-60,6-67,4 кГц.

Третьей особенностью телефонной сети является то, что она обладает большими возможностями по негласному внедрению устройств съема информации в различные её элементы, а также многообразными возможностями подключения их к ней, практически, в любом месте расположения телефонной линии не только в помещениях объекта поиска, т. е. около телефона или внутри его, в телефонной розетке, но и за пределами помещений объекта поиска (в коммутационной коробке, в телефонном шкафу, а в некоторых случаях, в телефонном колодце и даже на городской или офисной телефонной станции).

Четвёртой особенностью телефонной сети является то, что она, как было указано ранее, является источником конфиденциальных сведений, которые негласно могут передаваться не только по телефонной линии, но и используя телефонный радио ретранслятор передаваться по радиоканалу.

Исходя из вышеизложенных особенностей телефонной сети при визуальном её осмотре необходимо произвести тщательный осмотр всех элементов, начиная с телефонных аппаратов и кончая, если имеется такая возможность, офисной и городской телефонной станции. Следует отметить, что

телефонные колодцы и городские телефонные станции находятся в муниципальном обслуживании. Следовательно, осмотр этих элементов должен проводиться с разрешения руководства городской телефонной сети.

Особое внимание при обследовании элементов телефонной сети должно быть уделено проверке телефонного шкафа.

Для выявления возможного наличия в нём устройства съема информации необходимо произвести детальный визуальный осмотр плинтов и боксов, а также труб, в которых размещаются провода, ведущихся к абоненту. Провода из этих труб по возможности должны быть вытянуты и детально осмотрены как сами провода, так и полость внутри трубы.

После визуального осмотра элементов телефонного шкафа с помощью телефонного усилителя "ШПИЛЬ" или другого усилителя необходимо провести прослушивание сигналов в каждой телефонной линии, принадлежащей объекту поиска. С этой целью с помощью щупов изделия "ШПИЛЬ" произвести его подключение к соответствующим клеммам телефонного плинта. Подключение к телефонной линии телефонного усилителя не должно влиять на функционирование телефонной сети

Телефонный усилитель должен иметь следующие потребительские параметры:

- Диапазон частот анализируемых сигналов- 0.2-4.0кГц;
- Уровень анализируемых сигналов – 50-3000мВ;
- Вид подключения к телефонной линии –

гальванический.

Следует обратить внимание, что при отсутствии в телефонной сети сигналов телефонных переговоров или устройств съема информации в головных телефонах будут прослушиваться шумы линии, а при наличии в телефонной сети сигналов телефонных переговоров или сигналов устройств съема информации в головных телефонах будут слышны телефонные переговоры или акустические сигналы помещения объекта поиска, в том числе сигналы бытового радиоприёмника, установленного в одном из помещений объекта поиска.

Для локализации места размещения устройства съема информации в элементах телефонной сети можно воспользоваться изделиями «Шпагат» или «Пиранья».

При обследовании телефонной сети необходимо также проводить проверку на возможность наличия в ней радиотелефонных подслушивающих устройств. Такая проверка может быть произведена с помощью индикаторов поля "ШКАТУЛКА", "Д-006", "Д-008", "ИПф-6" и других подобных изделий, параметры которых не хуже параметров вышеназванных индикаторов поля. С этой целью необходимо установить телефонную связь с любым абонентом, например, набрав номер телефона 100, в это время поисковик с индикатором поля анализирует электромагнитное радиоизлучение перемещая его вдоль телефонного аппарата, розеток, телефонной линии, плинтов и других элементов телефонной сети, находящихся в помещении объекта поиска и, по возможности, возле него.

Практика поисковых исследований показывает, что наиболее вероятным местом внедрения радиотелефонных устройств съема информации

является телефонный шкаф.

Для достоверного определения наличия (отсутствия) в телефонном шкафу радиотелефонного устройства съема информации и локализации места его размещения целесообразно использовать индикатор поля "Д-006", "ШКАТУЛКА" и другие подобные изделия путём перемещения антенны вдоль элементов телефонного шкафа. Причём, чем ближе антенна индикатора поля к месту размещения радиотелефонного устройства съема информации, тем уровень звукового сигнала, проявляющегося в виде акустической завязки будет больше.

Проверка наличия радиотелефонного устройства съема информации в телефонном шкафу проводится как при телефонных переговорах, так и при их отсутствии.

При обнаружении в телефонной сети устройства съема информации дальнейшее действие поисковой бригады должно быть аналогичным ранее описанным в этом учебном пособии.

Поиск устройств съема информации в радиотрансляционной сети методически производится аналогичным образом, что и поиск их в других проводных коммуникациях, описанных ранее, за исключением того, что при обследовании радиотрансляционной сети необходимо учитывать её многопрограммность.

В Москве и Московской области используется три программы радиотрансляционного вещания. Сигналы первой программы занимают диапазон частот 300-4000 Гц, второй -74,6-81.4 кГц и третьей -108,6-115,4 кГц.

Следует отметить, что негласно снятые акустические сигналы объекта поиска могут

передаваться в диапазонах частот 4,0-74,6 кГц и 81,4-108,6 кГц, а также в диапазоне частот свыше 115,4 кГц.

Исходя из этого в процессе поисковых исследований радиотрансляционной сети особое внимание должно быть уделено анализу диапазона частот устройств съема информации.

Для определения наличия и локализации мест внедрения устройств съема информации в радиотрансляционной сети целесообразно использовать аппаратуру поиска "ШТУРМ", "ШПАГАТ", "ПИРАНЬЯ", "ШКАТУЛКА", "Д-006"и другую аппаратуру.

Методика проверки радиотрансляционной сети на наличие в ней, несанкционированно внедрённого устройства съема информации, а также использование вышеописанной аппаратуры в процессе поисковых исследований аналогична ранее описанной с учетом её особенности.

РАЗДЕЛ 8. ОБСЛЕДОВАНИЕ ЭЛЕМЕНТОВ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ

В элементы строительных конструкций (стены, потолочные перекрытия, пол, окна, водопроводные и теплопроводные коммуникации, вентиляционные каналы и т.д.) могут быть внедрены устройства съема информации или их элементы как в процессе строительства здания, его капитального или косметического ремонта, так и путём специального внедрения в процессе их эксплуатации.

Несанкционированное внедрение устройств съема информации или их элементов на объекте поиска может быть осуществлён также путём жесткого закрепления на поверхностях элементов строительных конструкций со стороны сопредельных помещений или путём дистанционного съема сигналов информации с их поверхностей. В последнем случае осуществляется беззаходный метод несанкционированного съема акустических сигналов объекта поиска.

Добыча информации путём внедрения устройств съема информации в процессе строительства здания, а также путём их закрепления со стороны сопредельных помещений рассчитано на несанкционированную добычу различных конфиденциальных сведений в течении длительного времени, а добыча информации путём внедрения устройств в процессе ремонта, а также путём дистанционного съема акустических сигналов объекта поиска рассчитана на добычу конкретных сведений в течении ограниченного времени (нескольких часов, нескольких суток).

Многообразие элементов строительных конструкций объектов поиска и возможных мест

внедрения в них устройств съема информации, а также особенности обследования различных категорий элементов строительных конструкций накладывает определённые требования на порядок их обследования, который в обобщённом виде целесообразно проводить в следующей последовательности.

Сначала необходимо обследовать ограждающие элементы строительных конструкций (стены, потолочные перекрытия, полы и т.д.), затем проводить обследование окон, вентиляционных каналов и в последнюю очередь проводить обследование теплопроводных и водопроводных коммуникаций.

Практика обследования оградительных элементов строительных конструкций показывает, что устройства съема информации и их элементы несанкционированно могут быть размещены за штукатуркой, под обоями, в их объемах и в других местах.

Особенности несанкционированного внедрения и размещения устройств съема информации в оградительных элементах строительных конструкций накладывает определённые требования к их обследованию.

Обследование стен, потолочных перекрытий, пола, окон и других оградительных элементов строительных конструкций объекта поиска начинается с визуального детального осмотра их поверхностей, используя лупы с разными коэффициентами увеличения. Причём, необходимо обращать внимание на наличие тёмных (светлых) пятен, которые могут быть связаны с внедрением устройств съема информации.

Визуальное обследование труднодоступных

мест оградительных поверхностей элементов строительных конструкций целесообразно проводить с использованием досмотрового комплекта "ШМЕЛЬ", описание которого приведено в 4 разделе настоящего учебного пособия.

После визуального обследования оградительных элементов строительных конструкций объекта поиска переходят к исследованию возможного наличия устройств съема информации в их объемах или на поверхности со стороны сопредельных помещений с помощью индикатора поля и нелинейного локатора.

С помощью индикатора поля могут быть обнаружены радио-подслушивающие устройства, находящиеся на объекте поиска и во включённом состоянии, а с помощью нелинейного локатора можно обнаружить любые устройства съема информации, содержащие в себе полупроводниковые приборы и находящиеся как на объекте поиска, так и внедрённые в соседние помещения в сопредельные элементы строительных конструкций в включённом и выключенном состояниях.

При обследовании оградительных элементов строительных конструкций в качестве индикатора поля могут быть использованы изделия "ШКАТУЛКА", "Д-006", "Д-008", "ИПФ-6"и другие, описание которых приведено в 4 разделе настоящего учебного пособия. В этом же разделе описаны правила их применения в процессе поисковых исследований.

В качестве нелинейных локаторов, как было сказано в 4 разделе настоящей книги, целесообразно использовать изделия "РОДНИК-2", "NR-900 ", "ОБЬ-1", "ШЛЮЗ" и другие.

Перед началом обследования оградительных элементов строительных конструкций с помощью

нелинейного локатора необходимо из всех смежных с проверяемым помещением, по возможности, убрать от обследуемых элементов всю аппаратуру и устройства, содержащие полупроводниковые приборы (магнитофоны, телевизоры, радиоприёмники, оргтехнику, телефонные аппараты и т.д.).

Затем осуществляют регулировку чувствительности нелинейного локатора для каждого оградительного элемента строительных конструкций. С этой целью, если это возможно, со стороны смежного помещения на обследуемый элемент закрепить полупроводниковый диод, транзистор или микросхему, а в обследуемом помещении включается нелинейный локатор и приёмопередающую антенну приближают вплотную к обследуемой поверхности и, уменьшая в нелинейном локаторе излучаемую мощность, добиваются минимального уровня, при котором он еще обнаруживает прикреплённый полупроводниковый прибор. Процедуру регулировки чувствительности необходимо осуществлять для каждого обследуемого элемента строительных конструкций.

После этого, перемещая приёмо-передающую антенну нелинейного локатора вдоль обследуемой поверхности со скоростью около 20м/с и медленно вращая её вокруг оси на 90 градусов, обследуют все ограждающие элементы строительных конструкций. При этом, при обнаружении в объеме элементов строительных конструкций устройств, содержащих полупроводниковые приборы в головных телефонах нелинейного локатора будет формироваться тональный звуковой сигнал.

При формировании тонального звукового сигнала в

головных телефонах нелинейного локатора подозрительные места обследуемых поверхностей фиксируются с помощью липкой ленты или другим способом, не оставляющим заметного следа.

Так предварительно обследуются все ограждительные элементы строительных конструкций одного помещения объекта поиска.

Затем приступают к детальному обследованию помеченных мест.

При этом следует иметь ввиду, что ряд помеченных мест могут быть ложными, образующиеся от находящихся в обследуемых элементах строительных конструкций арматуры, сетки рабицы, металлических труб и других элементов, ржавчина которых приводит к формированию полупроводникового эффекта. В следствии чего при облучении этих мест в головных телефонах нелинейного локатора формируется «дребежащий» звуковой сигнал, указывающий на наличие в них как бы устройств съема информации.

Для убеждения наличия (отсутствия) в помеченных местах устройств съема информации необходимо в момент обследовании постучать по обследуемой поверхности деревянным или резиновым молотком. Три этом, если в момент постукивании молотком в головных телефонах нелинейного локатора будет формироваться «дребежащий» звуковой сигнал, уровень и тональность которого не меняется, это указывает на наличие в анализируемом месте ложного полупроводникового прибора.

Для полной убеждённости наличия (отсутствия) в ограждительных элементах строительных конструкций устройств съема информации необходимо провести по вышеописанной методике визуальное и приборное обследование отмеченных мест, если такая возможность

имеется, с сопредельного помещения. Если и в этом случае прослушиваемый в головных телефонах звуковой сигнал является дребезжащим, то можно уверенно утверждать, что в обследуемом месте находится ложный полупроводниковый прибор.

Если при обследовании отмеченных мест с сопредельных помещений в головных телефонах нелинейного локатора также будет прослушиваться не «дребежащий» тональный звуковой сигнал, то можно с определённой уверенность сказать, что имеется подслушивающее устройство, которое может внедрено под отделочные материалы (обои, масляная краска, меловая побелка и т.д.), или оно внедрено на большие глубины.

Учитывая многообразие материалов строительных конструкций, отделочных материалов и сложность определение наличия устройств съема информации обследование ограждающих поверхностей элементов строительных конструкций объекта поиска должны осуществлять сотрудники поисковой бригады, обладающие большим опытом поисковых исследований и специализирующиеся по этому направлению.

На последнем этапе обследования оградительных элементов строительных конструкций переходят к оценке их потенциальных возможностей в качестве каналов утечки информации. С этой целью, по возможности, необходимо разместить в сопредельном помещении включенный бытовой радиоприёмник, а на ограждающей поверхности жестко закрепить имитатор электронный стетоскоп, позволяющий прослушивание акустических сигналов в сопредельных помещениях через оградительные элементы строительных конструкций.

Имитатор электронного стетоскопа должен

иметь потребительские параметры не хуже чем приведены ниже.

Диапазон частот анализируемых сигналов, кГц 0,3-3,4;

Допустимая толщина ограждающих элементов строительных конструкций, мм

для бетонных ограждений до 500;

для кирпичных ограждений до 300;

для деревянных ограждений до 100;

Продолжительность непрерывной работы, час до 15.

При обследовании ограждающих конструкций если в головных телефонах электронного стетоскопа будут прослушиваться акустические сигналы сопредельных помещений, следовательно через обследуемый оградительный элемент строительных конструкций можно негласно без захода на объект поиска снимать информацию, т.е. он может быть каналом утечки информации.

По результатам оценки возможных каналов утечки информации всех оградительных элементов строительных конструкций поисковая бригада вырабатывает организационные и технические рекомендации по их нейтрализации.

Обследование окон нужно осуществлять с учётом того, что устройства съема информации могут быть внедрены в рамы или в подоконник. Поиск устройств съема информации в окнах необходимо проводить сначала визуально, а затем с использованием аппаратуры (индикатора поля, нелинейного локатора и рентгеновского аппарата).

При этом необходимо обратить внимание, что обследование их осуществляется как при закрытом положении оконных рам, так и при открытом положении оконных рам на 90 градусов. Это позволит в процессе

поиска избавиться от паразитного излучения, которое может возникнуть в следствии наведения мощным телевизионным сигналом или радиостанцией на металлические элементы оконной рамы.

Методика обследования оконных рам с использованием индикатора поля, нелинейного локатора и рентгеновской аппаратуры проводится аналогично методике обследования оградительных элементов строительных конструкций, которая детально описана ранее.

При обследовании вентиляционных каналов следует учесть, что в вентиляционных каналах устройства съема информации могут быть внедрены в сопредельных с объектом поиска вент каналах, расположенных выше и ниже на несколько этажей. Поэтому необходимо произвести обследование всего вентиляционного, канала здания в котором размещается помещение объекта поиска.

Обследование вентиляционного канала проводится путём визуального осмотра его объема с помощью досмотрового комплекта "ШМЕЛЬ" с подсветкой узконаправленным фонарём.

По окончании визуального осмотра вентиляционного канала оценивается потенциальная его возможность по негласной передаче акустических сигналов из одного помещения в другое. С этой целью необходимо: во первых, разместить микрофон с усилителем низкой частоты в вентиляционном канале объекта поиска; во вторых, выключить на объекте поиска все радио и телевизионные приёмники и в третьих, прослушать с помощью головных телефонах акустические сигналы, имеющиеся в объеме вентиляционного канала.

Если в процессе оценки в головных телефонах будут прослушиваться акустические сигналы

сопредельных помещений, следовательно, вентиляционный канал может быть использован как канал утечки информации. В этом случае поисковая бригада показывает руководству объекта поиска наличие возможного канала утечки информации и даёт организационные и технические рекомендации по его устранению.

Обследование водопроводных и теплопроводных коммуникаций на объекте поиска можно проводить только лишь детальным визуальным осмотром всех батарей, труб и стояков.

Для оценки потенциальных возможностей водопроводных и теплопроводных коммуникаций по несанкционированному съему акустических сигналов объекта поиска необходимо, если есть такая возможность, датчики электронного стетоскопа жестко закрепить поочерёдно сначала на вводную, а затем выводную трубу во всех водопроводных и теплопроводных коммуникациях. При каждом закреплении датчиков электронного стетоскопа необходимо прослушать сигналы на головных телефонах и убедиться в их наличии (отсутствии).

Если в процессе изучения каналов утечки информации водопроводных и теплопроводных коммуникаций объекта поиска выясняется потенциальная возможность использования их для несанкционированной беззаходной добычи информации поисковая бригада показывает руководству объекта поиска наличие такого канала утечки информации и даёт рекомендации для его устранения.

При обнаружении в том или ином элементе строительных конструкций устройства несанкционированного съема информации

дальнейшие действия поисковой бригады должна проводиться в том порядке, как описано ранее.

РАЗДЕЛ 9. ПОДВЕДЕНИЕ ИТОГОВ ПОИСКОВЫХ ИССЛЕДОВАНИЙ

В зависимости от реализации мотивации поисковых исследований, от сложности и объема работ их осуществления, а также от полученных результатов оформление подведения итогов может быть разным.

По договорённости руководителей объекта поиска и поисковой бригады подведение итогов поисковой работы может быть осуществлено в письменном или в устном виде.

В обобщённом виде по окончании поисковых исследований могут быть подготовлены описание поисковых исследований и акт проведения поисковых исследований с предложением по нейтрализации возможных каналов утечки информации на объекте поиска.

Описание поисковых исследований подготавливается в произвольной форме, а объем работ и их содержание определяется договорённостью между руководителями объекта поиска и поисковой бригады.

Образец описания проведенной поисковой работы приведен в приложении 1.

В описание поисковых исследований могут входить:

- мотивация поисковых исследований, исходные данные о предполагаемом противнике, оперативная и техническая обстановка на объекте поиска и другие необходимые материалы;

- состав и состояние элементов строительных

конструкций, проводных, теплопроводных и водопроводных коммуникаций, предметов быта и интерьера и т.д.;

- способы и аппаратура, используемые в процессе поисковых исследований (с обязательным указанием основных потребительских параметров поисковой аппаратуры);

- электромагнитная обстановка на объекте поиска с указанием подозрительных спектральных составляющих или диапазона частот;

- способы оценки возможных каналов утечки информации и потребительские параметры используемой аппаратуры;

- перечень коммуникаций и мест, которые были подозрительными;

- способ и техническое средство, позволившие обнаружить несанкционированно внедренное устройство съема информации или были сняты подозрения на наличие их в отмеченных местах или в водопроводных и теплопроводных коммуникациях;

- характеристика возможных каналов утечки информации.

Одним из важных документов, отражающих основное содержание и результаты поисковых работ является акт поисковых исследований.

В акте поисковых исследований (возможный образец которого приведён в приложении 2) необходимо отразить:

- время и место проведения поисковых исследований;
- состав поисковой бригады;
- характеристику канала утечки информации, из

- которого изъято устройство съема информации (если такое устройство было найдено на объекте поиска);
- возможное место размещения пункта приёма сигналов информации;
- дальнейшее местонахождение изъятого устройства съема информации;
- потенциальные возможности системы несанкционированного съема информации;
- степень информационной защищенности объекта поиска по всем возможным каналам утечки информации;
- рекомендации по техническим средствам предотвращения негласного съема информации, которые необходимы объекту поиска для нейтрализации возможных каналов утечки информации.

Акт поисковых исследований оформляется в произвольной форме.

Третьим документом, подводящим итоги проведенной поисковой работы и предостерегающим возможность утечки конфиденциальной информации, является предложение по нейтрализации каналов утечки информации.

В предложении по нейтрализации каналов утечки информации на объекте поиска должны быть отражены:

- конкретный канала нейтрализации (элемент строительных конструкций, проводная коммуникация, тепло и водопроводная коммуникация и т.д.);
- рекомендуемое устройство защиты информации и его основные потребительские параметры, обращая особое внимание на степень

информационной защиты, место внедрения устройств информационной защиты;

- ориентировочные финансовые затраты по обеспечению технической защиты негласного съема информации;
- необходимое время для оборудования системой защиты информации.

В некоторых случаях в процессе подготовки к проведению поисковых исследований по договорённости руководства объекта поиска и поисковой бригады вся работа оканчивается устным сообщением о проведенной работе. В этом случае руководитель поисковой бригады докладывает руководству объекта поиска о проделанной работе, способах поиска и использованной аппаратуре.

В этом случае при обнаружении устройства съема информации руководитель поисковой бригады устно или письменно, в зависимости от пожеланий руководства объекта поиска, докладывает им о найденном устройстве, о методе и способе его внедрения и о его возможных основных потребительских параметрах (канал утечки информации, основные электрические характеристики, ориентировочная дальность передачи сигналов информации, ориентировочное время внедрения и т.д.). Кроме этого он информирует руководство о состоянии информационной защищённости объекта поиска, возможных каналах утечки информации и путях их нейтрализации.

После детального обсуждения полученных результатов руководитель поисковой бригады вместе с руководством объекта поиска решают вопрос по дальнейшему использованию найденного устройства съема информации и необходимом и достаточном объеме выполненных работ.

Приложение 1

ОПИСАНИЕ ПРОВЕДЕНИЯ ПОИСКОВЫХ ИССЛЕДОВАНИЙ

Поисковые исследования по обнаружению устройств съема информации проводились в соответствии с методикой поисковых исследований [4J, разработанной ЗАО ЩИТ, которая опробована во многих коммерческих организациях в период с 1992 по 1998 гг.

В процессе поисковых исследований осуществлялись следующие работы:

1. Проводился визуальный осмотр всех помещений объекта поиска и сопредельных с ним мест, предметов быта и интерьера, элементов абонентской и офисной телефонной сети, элементов электросети, вентиляционного канала, теле и радиоаппаратуры.

Для визуального осмотра использовались комплект аппаратуры "ШТУРМ", досмотровый комплект "ШМЕЛЬ-2", набор луп и другие средства и приспособления.

2. Осуществлялась оценка наличия сигналов устройств негласного съема информации в абонентской и офисной телефонной сети, в электросети, в радиотрансляционной сети, в линиях пожарной и охранной сигнализации и в других проводных коммуникациях. С этой целью использовался комплекс для обнаружения подслушивающих устройств в проводных коммуникациях "ШПАГАТ".

Проверялось наличие[98]в осматриваемых помещениях, в автомашине или на открытой местности и расположенных в них радио-

подслушивающих устройств съема информации. Для определения наличия (отсутствия) радиоподслушивающих устройств использовался индикатор поля "ШКАТУЛКА".

4. Исследование электромагнитной обстановки во всех обследуемых местах и предметах быта и интерьера, в приборах и устройствах, находящихся на объекте поиска. Измерение проводилось с помощью комплекса автоматизированного радиоконтроля "АРК-ПА2".

5. Осуществлялась разборка всех элементов проводных коммуникаций (выключателей, розеток, коммутационных коробок, телефонных аппаратов, радиотрансляционных приёмников и других приборов, и устройств, находящихся на объекте поиска). Для разборки и осмотра элементов и устройств телефонной радиотрансляционной, электросетевой и другой аппаратуры использовалась аппаратура инструменты, имеющиеся в комплекте «Штурм».

6. Обследовались пол, потолочные перекрытия, стены, вентиляционные каналы на наличие в них устройств съема информации. Для обследования элементов строительных конструкций использовались металлоискатель "ХМД-02" и нелинейный локатор "ШЛЮЗ".

В результате комплексных исследований на объекте поиска на момент проверки было обнаружено (не обнаружено) устройство съема информации с указанием конкретно, где, когда и какое устройство было найдено и его основные потребительские параметры, а также проведена оценка возможных каналов утечки информации.

Для предотвращения негласного съема

конфиденциальной информации по всем возможным каналам утечки информации

целесообразно использовать изделия "ШТАНГА", "ШПАГА, "ШУРФ" и т.д.

Для обеспечения фиксации работы в обследуемых местах объекта поиска радиоподслушивающих устройств целесообразно использовать мобильный или стационарный обнаружитель радиоподслушивающих устройств ("ШКАТУЛКА", "ШЛЕМ").

Поисковые исследования выполнены в полном объеме.

Приложение 2

Согласен	Утверждаю
Руководитель организации объекта поиска	Руководитель организации поисковой бригады
«____» 2010 г.	«____» 2010 г.

АКТ

ПРОВЕДЕНИЕ ПОИСКОВЫХ ИССЛЕДОВАНИЙ

" " 2010 г. бригада сотрудников "Организации" в составе ----------

_____

_____ в присутствии сотрудников объекта поиска «Организации»_____

_____ провела поисковые исследования в помещениях (в автомашине, на открытой местности).

Поисковая работа проводилась в соответствии с договором, заключенным между Исполнителем (поисковой бригады) «Организация» и ЗАКАЗЧИКОМ «Организация».

В ходе поисковой работы осуществлялась:

- проверка элементов строительных конструкций (потолочных перекрытий, стен, пола, окон, вентиляционных каналов и водопроводных и теплопроводных коммуникаций);

- проверка абонентской телефонной сети, состоящей из

телефонных линий, из- телефонных аппаратов, из---- - розеток;

- проверка офисной телефонной сети, состоящей из ----------

телефонных линий, из ---телефонных аппаратов, из ---розеток;

- проверка электросети, состоящей из ---фаз, из ---светильников, из ---настольных ламп;

- проверка электронных приборов (телевизоров--------шт, радиоприёмников --- шт., персональных компьютеров ----шт., электронных часов --- шт.;

- обследование предметов быта и интерьера;

стулья ----------шт., столы----- шт., тумбочка------ шт., стенной шкаф --- шт., вазы-------шт., цветы--------шт.;

- разборка элементов телефонной сети; разборка элементов электросети;

-измерение электромагнитной обстановки;

-проверка автомашины (марка машины);

-проверка на открытой местности (характеристика).

В процессе поисковых исследований использовались:

- комплект аппаратуры для поиска, обнаружения и изъятия устройств съема информации "ШТУРМ";

- комплекс для обнаружения устройств съема информации в проводных коммуникациях "ШПАГАТ";

- индикатор электромагнитных излучений "ШКАТУЛКА";

-обнаружитель устройств съема информации в линии электросети "ШТР АФ";

- фиксатор устройств съема информации в телефонной сети

"ШПИЛЬ";

- досмотровый комплект "ШМЕЛЬ-2".

Выводы.

1. Поисковая бригада установила:

-на момент поисковых исследований на объекте поиска обнаружены, где конкретно, краткая характеристика устройства съема информации) или не обнаружено.

2. С целью устранения потери конфиденциальной информации в последующем целесообразно:

- оборудовать объект поиска следующими техническими средствами информационной безопасности (по элементам строительных конструкций, по проводным коммуникациям, по водопроводным и теплопроводным коммуникациям и другим возможным каналам утечки информации);

- не реже двух раз в год проводить комплексные поисковые исследования.

3. Работа выполнена в полном объеме и в соответствии с Договором подлежит оплате.

Члены поисковой бригады

ЛИТЕРАТУРА

1. Алешенков М., Бузанова Я., Ярочкин В. Концепция комплексной безопасности предпринимательства: Учебное пособие. – М.: Паруса, 1997 - 31с.

2. Ярочкин В. И. Безопасность информационных систем. – М.: Ось – 89, 1996. –320 с..

3. Шаповалов П. П. Методика поисковых исследований . М,: ЗАО «ЩИТ» .1995-48 с.

4. РД ГТК. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации. - М.: Военное издательство, 1992 г.

5. РД ГТК. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. - М,: Военное издательство, 1992 г.

6. РД ГТК. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. – М,: Военное издательство, 1992 г..

7. РД ГТК. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Термины и определения. – М, : Военное издательство, 1992 г.

8. Белая книга Российских спецслужб. Изд. 2- е. – М,: Информационно – издательское агентство «Обозреватель», 1996 – 272 с.

9. Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия. – _М,: Право и закон, 1996 - 182 с.

10. Галатенко В. А. Информационная безопасность // Открытые системы. – 1996.–№ 3 - с. 42-45 .

11. Галатенко В.А. . Информационная безопасность // Открытые системы. – 1996.–№ 3 - с. 53-57.

12. Галатенко В. А. Информационная безопасность // Открытые системы. – 1996.–№ 3 - с. 40-47

13. Галатенко В. А.91 Информационная безопасность: Обзор основных положений . | |Jet Info – 1999.—Спец. выпуск.—60 с.

14. Хореев А. А. Технические средства и способы промышленного шпионажа. Учебное пособие. - М.: ЗАО «Дальснаб, 1997-230 с.

15. Лунегов А, Н., Рыжов А. Л. Технические средства и способы добывания и защиты информации._- М. : ВНИИИ «Стандарт», 1993-95 с.

16. Брусницын Н. А. Открытый шпионаж.- М,: Воениздат, 1999 – 56 с.

17. Миронычев С. К. Коммерческая разведка и контрразведка или промышленный шпионаж в России и методы борьбы с ним. М. "ДРУЖОК", 1995 г.

18. Ярочкин В. И. Предпринимательство и безопасность. ч,1. Несанкционированный доступ к источнику конфиденциальной информации.-М.: Экспрессное бюро, 1994 г.

19. Шаповалов П. П. Практическое руководство по поиску устройств съема и передачи информации. М. ЗАО "ЩИТ". 1996 г.

20. Шаповалов П.П. Коммерческий технический шпионаж и пути его нейтрализации. М. ЗАО "ЩИТ". 1999 г.

21. Атакующая спецтехника фирмы

Св. план 2010 г., поз.277
Шаповалов Пётр Павлович
Поиск и оперативное пресечение
несанкционированного съема информации
Учебное пособие

Подписано в печать - 15.04.10. Формат 60×84/16
Усл . п.л. - 6,75. Заказ № 248. Тираж 100 экз.

127994, Москва, ул. Образцова, д.9, стр.9
Типография МИИТ