GAUDEAMUS

УЧЕБНО-ПРАКТИЧЕСКОЕ ПОСОБИЕ

для военных специальностей

С.Н. КОЗЛОВ

# ЗАЩИТА ИНФОРМАЦИИ

## УСТРОЙСТВА НЕСАНКЦИОНИРОВАННОГО СЪЕМА ИНФОРМАЦИИ И БОРЬБА С НИМИ

ПЕРВЫЕ СРЕДИ РАВНЫХ

С.Н. Козлов

*Учебно-практическое пособие*

# ЗАЩИТА ИНФОРМАЦИИ

## УСТРОЙСТВА НЕСАНКЦИОНИРОВАННОГО СЪЕМА ИНФОРМАЦИИ И БОРЬБА С НИМИ

«Академический проект»
Москва, 2018

УДК 342; 343; 004; 351/354
ББК 67.400; 67.408; 32.97; 67.401
К 59

**Козлов С.Н.**

К 59 Защита информации: устройства несанкционированного съема информации и борьба с ними: Учебно-практическое пособие. — 2-е изд. — М.: Академический проект, 2018. — 286 с. — (Gaudeamus).

ISBN 978-5-8291-2174-7

Настоящее учебно-практическое пособие подготовлено на основе многолетнего практического опыта ветеранов отечественных спецслужб, специализирующихся на обеспечении безопасности высшего руководства страны и борьбе с терроризмом.

Благодаря представленным в пособии материалам читатель не только сможет ознакомиться с каналами утечки информации, устройствами ее несанкционированного съема (УНСИ) и тактикой преступных элементов при установке и контроле этих устройств, но и получит наглядный и эффективный практикум по организации поиска и локализации УНСИ.

Книга написана простым и доступным для понимания языком, содержит большое количество иллюстраций, что делает ее полезной не только для специалистов в области обеспечения безопасности и работников профильных учебных заведений, но и для широкого круга читателей, чей бизнес предполагает острую конкурентную борьбу.

Пособие рекомендовано Учебным центром Содружества телохранителей России «Железный орел».

**УДК 342; 343; 004; 351/354**
**ББК 67.400; 67.408; 32.97; 67.401**



ISBN 978-5-8291-2174-7

# Предисловие

Все тайное рано или поздно становится явным.
*Сократ*

Данная книга будет посвящена защите информации. Для успешной реализации преступной акции противнику надо знать в основном три вещи: время, место и способ нападения. Чтобы выяснить эти моменты, ему приходится собирать информацию о сотрудниках компании, главным образом о руководстве, их привычках, местах проживания и работы, окружении, включая не только родственников, но и друзей, партнеров, сослуживцев, любовниц и прочих. Очень важное значение уделяется системе безопасности и конкретным персоналиям, причем часто не руководству, а сотрудникам, обеспечивающим непосредственную защиту, — телохранителям, охранникам, техникам. Руководитель службы безопасности может быть семи пядей во лбу, но на рубеже атаки все равно стоит не он, а конкретный сотрудник. Поэтому именно от того как этот сотрудник несет службу, в основном и зависит, атакуют компанию или нет, и если да, то как.

Для сбора информации преступники могут использовать разные способы. В ход идет все: Интернет, средства массовой информации, наружное наблюдение, специальные технические средства и т. д.

Поскольку в России основная масса нападений на владельцев и руководителей организаций происходит на маршрутах движения и около мест постоянного или временного пребывания то сбор информации для преступников часто оканчивается на этапе наружного наблюдения. Как противодействовать «наружке» мы подробно рассмотрели в книге «Наружное наблюдение», но поскольку противник в зависимости от ситуации не всегда ограничивается наружным наблюдением, то сотрудникам безопасности необходимо быть готовым к столкновению и с другими способами сбора информации. Вам необязательно уметь пользоваться нелинейным локатором, но знать, что это, как выглядит и каковы его возможности, вы обязаны. Не секрет, что не везде существуют команды техников, которые занимаются поиском и закрытием каналов утечки информации. Достаточно часто для периодических проверок таких специалистов приглашают со стороны. Кто должен проверить качество их работы? Правильно. Эту задачу клиент повесит на руководство безопасности. А те в свою очередь на подчиненных, обычно на телохраните-

лей, старших охраны объектов, а то и простых охранников: они же последний рубеж обороны. И что этот «рубеж» будет делать в этом случае? Опять же правильно. Будет стоять и хлопать глазами. В большинстве случаев. Уж об этом я могу сказать с уверенностью. Через руки преподавателей нашей организации за пятнадцать лет существования прошла минимум четверть телохранителей г. Москвы. Так что информацией, где что умеют и где как учат, мы владеем полностью. Первичных знаний и навыков по защите информации, особенно в низовом звене, нет почти ни у кого. А ведь именно знание возможностей и тактики действий противника в конечном итоге определяет нашу с вами тактику предупреждения, или пресечения нападения.

Нужны ли эти знания рядовому сотруднику? Давайте рассуждать. Если на этапе разведки противник будет прослушивать телефон клиента, то он запросто сможет узнать, где и когда он будет находиться. Вам важно не допустить утечки этой информации? Конечно же да. Но как? Ведь для этого необходимо не просто знать о том, что вас могут подслушать. Надо знать, какие модели телефонов прослушать легче, какие модели прослушать нельзя или сделать это затруднительно, могут ли вашего клиента идентифицировать по голосу в случае смены телефона и как быстро. И еще много чего другого.

Все может быть и проще. Например, секретарь руководителя имеет «добрую» привычку рассказывать по телефону любому позвонившему о том, где он находится. К счастью, экземпляры, которые все рассказывают вплоть до адреса и телефона, встречаются редко. Но все же встречаются. Однако это мало что меняет. В час «икс» вполне будет достаточно обычной фразы: «Иван Иваныч еще не приехал» или «Он сказал, что будет через десять минут». Этого хватит, чтобы свести, к примеру, на нет работу ваших ложных кортежей и дать информацию противнику об истинном месте нахождения клиента.

Следует также помнить, что невозможно искать то, чего никогда не видел и, более того, даже не представляешь, как это выглядит. Невозможно найти жучок, если ты не представляешь, что это такое и где он может устанавливаться. Вы вряд ли обратите внимание на электронный стетоскоп, даже если он будет находиться у вас под носом, если вы никогда с ним не сталкивались. И чтобы избежать таких недоразумений, надо иметь соответствующие знания.

Еще один немаловажный аспект в работе — это коммерческая тайна. В силу специфики своей работы сотрудникам безопасности приходится присутствовать на деловых встречах, конфиденциальных переговорах. Вы будете видеть и слышать то, о чем распростра-

няться не стоит. Эта информация запросто может нанести урон как репутации клиента, так и его бизнесу. Одно неудачно сказанное слово — и сделка на миллионы долларов летит к черту. И если даже защита информации не ваша основная задача, вряд ли вас погладят по головке, если узнают, что вы болтаете налево и направо о делах клиента, либо, наоборот, помалкиваете о том, что об этом болтает кто-то из ваших коллег. Что задумались о «стукачестве»? А как вы хотели? Безопасность понятие широкое.

И докладывать информацию, способную нанести ущерб безопасности охраняемых лиц, вы обязаны. Какой вам прок от клиента, которого не убили, но разорили? Точно. Никакого. Новое место работы искать придется. Так что его успех — это и ваш успех. И если его успех сегодня зависит от вас, то своевременно довести информацию до клиента ваш долг.

Однако стоит помнить, что информацию нужно донести нужную. Иначе вы рискуете превратиться именно в стукача, который бегает закладывать товарищей: мол, Петька сказал, что вы лох, потому что у вас галстук не того цвета. А вот для понимания того, что важно, а что нет, о чем говорить можно, а о чем нужно помалкивать, и нужно знать, какие сведения относятся к коммерческой тайне. Неплохо также представлять и что вам будет, если вы будете болтать не по делу. Для многих болтунов и невдомек, что по ряду моментов можно заработать тюремный срок.

Подводя итог сказанному, хочется заметить, что безопасность охватывает очень широкую область знаний и умений, и защита информации занимает там не последнюю роль.

# Глава 1. Информация, которую мы защищаем

## Введение

Для начала нужно разобраться, какую именно информацию нам предстоит защищать.

Выделяют две основные группы информации (см. рис. 1), подлежащие защите:

1) информация, которую противник может использовать для нанесения вреда жизни и здоровью сотрудников компании, например, организовать покушение на владельца компании или ключевых работников;
2) информация, которая может разрушить бизнес компании.


*Рис. 1*

Утечка информации из группы № 2, как вы уже, наверное, догадались, не только может оставить нас с вами без работы, но и серьезно подорвать здоровье владельцев и руководителей организации, вплоть до смертельного исхода. Рассмотрим указанные группы подробнее.

### 1.1. Информация, необходимая для нанесения вреда жизни и здоровью сотрудников компании

Какую информацию будет собирать противник при организации покушения?

Противника интересует, где, когда и как удобнее и желательно с минимальными затратами совершить нападение. Для этого ему по-

надобятся установочные данные объекта нападения, то есть фамилия, имя, отчество, адрес места жительства и места работы, данные на личный автотранспорт, состав семьи, номера телефонов. Кроме того, преступников будет интересовать окружение данного лица, состояние его здоровья, его привычки и характер, личные привязанности, хобби и т. д. О состоянии его безопасности я уже и не говорю. Кто руководит охраной? Как она организована и оснащена? Какие тактические приемы использует? Каково состояние дисциплины в каждой смене охраны? Как подготовлены охранники? Эти и многие другие вопросы очень интересуют противника. Ответив на них, он и получит в итоге искомые: где? когда? и как?

Как видите, в эту группу в основном входит информация о частной жизни объекта покушения и информация о состоянии системы безопасности, т. е. информация для служебного пользования, или служебная информация. К сожалению, мы не можем придать ей грифа «Секретно» или «Совершенно секретно». Поэтому хотим мы того или нет, защитить этот блок информации на 100% мы не сможем. Но стремиться к этому, как вы сами понимаете, надо.

Правовую основу для защиты этой информации составляют Конституция РФ (ст. 23—24), Закон «О защите персональных данных», Кодекс РФ «Об административных правонарушениях» (ст. 13.11) и Уголовный кодекс РФ (ст. 137 и 138, 272 и 273).

Что можем мы почерпнуть для себя из этих законов?

**Статья 23. Конституции РФ гласит:**

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

**Статья 24. Конституции РФ гласит:**

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

**Федеральный закон «О персональных данных»** конкретизирует, что именно представляют собой персональные данные (см. При-

ложение 1). Статья 3 этого закона определяет, что персональные данные — это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. По сути своей под персональными данными понимается установочная информация, о которой мы говорили выше.

Закон также определяет принципы и условия обработки персональных данных. Разъясняет, какая информация и когда является общедоступной. Устанавливает ответственность за разглашение указанной информации.

Какая именно ответственность грозит тем, кто незаконно использует установочную информацию, определяется в Кодексе «Об административных правонарушениях» и Уголовном кодексе.

**Статья 13.11. КоАПП**

**Нарушение установленного законом порядка сбора, хранения, использования и распространения информации о гражданах (персональных данных)**

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) — влечет предупреждение и наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц — от пяти до десяти минимальных размеров оплаты труда; на юридических лиц — от пятидесяти до ста минимальных размеров оплаты труда.

**Статья 137. УК РФ**

**Нарушение неприкосновенности частной жизни**

1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации — наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права

занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2. Те же деяния, совершенные лицом с использованием своего служебного положения, — наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

**Статья 138. УК РФ**

**Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений**

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан — наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.
2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, — наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок от одного года до четырех лет.
3. Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, — наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

**Статья 272. УК РФ**
**Неправомерный доступ к компьютерной информации**

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, — наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

**Статья 273. УК РФ**
**Создание, использование и распространение вредоносных программ для ЭВМ**

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами — наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются лишением свободы на срок от трех до семи лет.

Как видите, большинство указанных статей грозят людям, занимающимся сбором информации об охраняемом лице, либо тем, кто эту информацию разглашает, в основном денежными штрафами.

Размеры этих штрафов в сравнении с возможной суммой взятки за разглашение нужных противнику сведений плевые. Именно поэтому указанные статьи на практике не работают. К тому же факт умышленного разглашения еще нужно доказать, а это дополнительный повод к тому, что в суде практически нет дел по данным статьям, за исключением ст. 272 и 273 УК РФ. Хотя и здесь что-то делается только потому, что иностранцы сильно обеспокоены борьбой с «хакерами», а наша страна стремится в ВТО, иначе правоохранители и в этом направлении особенно бы не дергались. Притом не факт, что в вашем частном случае вам придут на помощь. Одно дело государство, а другое предприниматель Иванов.

Поэтому надеяться на страх людей перед законом не приходится, а потому защитить информацию в превентивном порядке, опираясь только на законы, не получится.

## 1.2. Информация, необходимая для нанесения ущерба или разрушения бизнеса компании

К данной группе информации в основном относятся сведения, составляющие коммерческую тайну.

> **Коммерческая тайна** — это конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (ФЗ «О коммерческой тайне»).

Информация, составляющая коммерческую тайну — научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, в отношении которой обладателем такой информации введен режим коммерческой тайны.

**Коммерческую тайну могут составлять:**

1. Предпринимательская информация: финансовые сведения; деловые планы и планы производства новой продукции; списки клиентов и продавцов; контракты; маркетинговые исследования; организационные схемы; характеристики на сотрудников и т. д.
2. Техническая информация: научно-исследовательские проекты; сведения о секретах технологии производства продукции и ее технические параметры; заявки на патенты; программное обе-

спечение для ПК; химические формулы; эффективность и возможности производственных методов; оборудования и систем и т. д.

3. Информация об организационных особенностях предприятия: сводные данные о сотрудниках, и особенно о лицах, принимающих ключевые решения; социально-психологические характеристики лиц, принимающих ключевые решения; программы расширений и приобретений; главные проблемы фирмы и возможности для их решения; программа проведения научно-исследовательских работ и т. д.
4. Информация о системе экономической безопасности предприятия: сведения о способах, силах и средствах обеспечения безопасности, технических средствах охраны и местах их расположения; сведения о руководстве безопасности, их связях; и т. д.

**При этом не могут согласно закону составлять коммерческую тайну следующие сведения:**

1. Содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры.
2. Содержащиеся в документах, дающих право на осуществление предпринимательской деятельности.
3. О составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов.
4. О загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом.
5. О численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест.
6. О задолженности работодателем по выплате заработной платы и по иным социальным выплатам.
7. О нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений.

8. Об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности.
9. О размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации.
10. О перечне лиц, имеющих право действовать без доверенности от имени юридического лица.
11. Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Вот теперь-то мы с вами сможем определить, о чем можно говорить, а о чем нельзя. Но опять же, применять санкции в отношении других возможно, если только в вашей организации официально введен режим коммерческой тайны и в трудовом договоре работников присутствует пункт о неразглашении. Иначе ваши сослуживцы и персонал предприятия могут заливаться соловьем о секретах вашей организации — по закону им ничего не будет.

Кстати, о законе. Правовую основу коммерческой тайны составляют: Конституция РФ, Закон «О коммерческой тайне» (см. Приложение 2), УК РФ (ст. 183).

Что говорит Конституция и Закон «О коммерческой тайне», мы видели выше, а более подробно с положением законов вы можете ознакомиться в приложениях. А вот какую ответственность за разглашение коммерческой тайны предусматривает УК, надо рассмотреть внимательнее.

**Статья 183. УК РФ**

**Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну**

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом — наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.
2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, — наказываются штрафом

в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, — наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.
4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, — наказываются лишением свободы на срок до десяти лет.

Ничего странного не замечаете? А дело вот в чем. Опираясь на УК, при желании можно запросто отправить за решетку и тех, кто разглашает, и тех, кто выведывает секреты вашей фирмы.

Беда лишь в том, что в нашем государстве все вечно с ног на голову ставится. Согласитесь, смешно, когда за сведения, приводящие к смерти человека, хотя по Конституции у нас человеческая жизнь — высшая ценность, тебя только оштрафуют. А вот за сведения, грозящие экономическим крахом, — посадят. Вот и получается, что цена человеческой жизни — копейка. Или, точнее, цена копейки — чья-то жизнь.

Но вернемся к делу. Теперь, когда мы более или менее разобрались с тем, что мы защищаем, пора разобраться и с тем, как конкретно информация утекает от нас к противнику. А для этого нужно понять, какие каналы утечки информации существуют и каков механизм получения сведений по этим каналам.

# Глава 2. Каналы утечки информации

Говоря о каналах утечки информации, следует помнить, что на сегодняшний момент среди специалистов в области защиты информации нет их единой классификации. В ряде случаев один и тот же канал имеет в разных источниках разные названия. Поэтому предлагаемая нами классификация не является окончательной или единственно верной. Во всяком случае, я с моими коллегами не претендую на звание последней инстанции, глаголющей истину. Просто мы считаем, что данный вариант классификации более понятен, чем ряд других.

Итак, основными каналами утечки информации являются:

- Люди.
- Вещественно-материальный канал.
- Технические каналы.

Каждый из этих каналов имеет свои особенности. Поэтому для получения информации по ним противник применяет различную технику и тактику, исходя именно из особенностей, присущих каждому конкретному каналу. Чтобы понять, что и как он будет делать, нам придется рассмотреть каждый канал повнимательнее.

## 2.1. Главный канал утечки информации – люди

Человеческий фактор во все времена оставался решающим в любой деятельности, а уж в безопасности особенно. Недаром старик Макиавелли писал, что только те средства обеспечения безопасности хороши, надежны и долговечны, которые зависят от вас самих и вашей собственной энергии. Читай — доверять нельзя никому. В эпоху СССР два ключевых лозунга — «Кадры решают все!» и «Болтун — находка для шпиона» — как нельзя лучше характеризовали состояние дел в рассматриваемом нами канале утечки информации. Если у тебя не лучшие сотрудники, то рано или поздно они начнут болтать языком. Конечно, в силу разных причин. Кто-то будет хвастаться, кто-то недовольно бубнить, но суть от этого не меняется. А поскольку будут болтать, то рано или поздно посторонние уши для их болтовни найдутся, со всеми вытекающими отсюда негативными последствиями.

В зависимости от группы, к которой принадлежит болтун, можно разделить людской канал на канальчики поменьше.

Людские (человеческие) каналы утечки информации:
- руководитель (владелец);
- родственники руководителя (владельца);
- друзья и знакомые руководителя (владельца);
- персонал компании (включая сотрудников безопасности);
- представители сторонних организаций (деловые партнеры, сотрудники правоохранительных органов и спецслужб, лечащие врачи, фитнес-инструкторы и т. д.).

Утечка по людским каналам может быть умышленной, неумышленной и вынужденной.

В случае умышленного разглашения сведений имеют место возмездная и безвозмездная передача сведений. Например, если уволенный охранник, обидевшись на охраняемое им лицо, расскажет противнику все об обеспечении его безопасности, получая при этом моральное удовлетворение, то такая форма передачи является безвозмездной. Если же он сделает это за деньги в результате подкупа — то это, понятно, возмездная форма. Но определяющим фактором здесь все равно является личное желание сотрудника, то есть умысел.

При неумышленной утечке информации болтун просто не осознает, что его болтовня может нанести ущерб фирме. Яркий пример такой утечки — так называемые «семейные болтуны». Большинству людей дома элементарно не о чем поговорить. А что вы хотели? Дом — работа. Работа — дом. О чем говорить-то? Вот и рассказывает человек о том, что творится на работе. Понятно, что приукрашивает все, что касается себя любимого, перед женой выпендривается, но все равно рассказывает. Но ведь это жена, близкий человек. А больше никому и ничего. Но на его беду, жена идет к подругам, а то и к любовнику и тоже рассказывает «последние новости» с работы своего благоверного. Те в свою очередь своим друзьям и знакомым и так до тех пор, пока информация не попадет к заинтересованным лицам. А уж попадет она обязательно. Будьте уверены. Хотя и нет в действиях источника информации злого умысла.

Ну и наконец третий вариант утечки — вынужденный. Это когда из носителя информации ее достали путем угроз, шантажа или банально «выбили». Можно по-разному относиться к данной ситуации. Но надеяться на то, что сопливая девчонка секретарь не скопирует нужный конкурентам документ, если накануне ее в темном подъезде зажали два здоровых амбала и пообещали облить кислотой, не приходится. Ваши сотрудники не будут рисковать своей жизнью или жизнью своих родственников ради ваших секретов. Им проще работу сменить. И если вы не смогли обеспечить их безопасность — это не их, а ваши проблемы. В моей памяти еще свежа

ситуация 1998 года, когда в одной известной компании у начальника юридического управления украли жену. В обмен на ее освобождение неизвестные требовали предоставить сведения о ряде договоров с зарубежными компаниями, естественно, неофициальных. Юрист повел себя, как герой, послал вымогателей подальше. Видимо, он просто не верил в серьезность намерений похитителей. Ведь он трудился в крутой организации. И что в итоге? А в итоге жену он получил по частям. И дальше по накатанной — запил, уволился из компании и куда делся дальше — одному богу известно.

Короче, верить на 100% нельзя никому. Человека можно загнать в такие рамки, что все равно расскажет, что надо. Старая поговорка о том, что у сотрудника безопасности нет друзей, а есть только враги, в контексте защиты информации отнюдь не лишена смысла. Ведь даже сам владелец бизнеса и то может оказаться каналом утечки информации. Сболтнул лишнего на переговорах и всё — ваши не пляшут. Вернее, не пляшут в основном его, но в итоге и ваши тоже. Не стоит надеяться и на родственников. В некоторых известных семьях отношения такие, что бразильские сериалы отдыхают. Слив информации друг о друге, бывает, идет аж через СМИ. Последний скандал в благородном семействе Слуцкеров (г. Москва) лишнее тому подтверждение. Не отстают и партнеры по бизнесу, которые норовят прибрать все в свои руки. Так в бытность поссорились бывшие друзья, а ныне непримиримые противники олигархи Прохоров и Дерипаска. Последний повел себя с товарищем по бизнесу, мягко скажем, некорректно.

Но все же один из главных каналов утечки информации — это персонал фирмы.

Даже с помощью технических приемов и засылки мнимых клиентов из компании утекает не так много информации, как от ее же собственных сотрудников. По оценке начальника отдела информационных систем Газпромбанка Игоря Кадощука, 70% утечек конфиденциальной информации из компаний уходит через персонал. «Зачем придумывать сложные схемы, если любые данные можно просто купить у сотрудников, особенно у малооплачиваемых», — констатирует он.

Можно и просто «вытащить» из чужих работников информацию под прикрытием разных легенд. Например, под видом приглашения на новую работу или, наоборот, заслав своего сотрудника на собеседование к конкуренту. Иногда разведчик может замаскироваться даже под журналиста, желающего взять интервью у топ-менеджера. Но сам он считает эти приемы сложными и малоэффективными — на его взгляд, они не дают точной информации.

Защитить от внутренней угрозы может только постоянная работа с персоналом, утверждают эксперты. Бизнесмены, согласно исследованию On Conference, считают самым эффективным способом предотвращения утечек разграничение уровней доступа к информации в соответствии со служебным положением. Так думают 60% респондентов. На втором месте по популярности — «повышение лояльности персонала к собственной компании» (40% респондентов). Еще 27% считают, что лучшей защитой является доверие к персоналу, а 20% — ограничение возможности копирования информации. Такое же количество высказалось в пользу просмотра личной и служебной почты сотрудников, 13% опрошенных признались, что в их компаниях прослушиваются телефонные разговоры, а 2% — что у них используется детектор лжи.

Подавляющее большинство респондентов заверяют, что лучший метод укрепления лояльности сотрудников — материальный. Зарплаты ниже средних по рынку повышают вероятность появления «крота». Важны и моральные поощрения, «пропаганда корпоративного духа» и помощь сотрудникам в решении их личных проблем. На наш взгляд, методы «положительной» мотивации в ряде случаев более эффективны, чем ограничения. Тем более что в России привыкли обходить любые запреты. Ведь если в компании запрещено пользоваться ICQ, отключена электронная почта или ограничен доступ в Интернет, сотрудники могут тайком подключать к компьютеру внешний модем. А он уже откроет для промышленных шпионов удобное «окошко» в локальную корпоративную сеть.

Другую потенциальную лазейку для разведчиков создают неаккуратные сотрудники, они выдают не меньше информации, чем предатели. Например, во многих офисах накопившиеся за день бумаги не уничтожают, а просто выбрасывают. Если собрать мусор хотя бы за один день, можно обнаружить много интересного — телефоны клиентов, внутренние распоряжения или схемы.

Это подтверждает пример инвестиционной компании «Вашъ финансовый попечитель». Ее директор по стратегическому развитию Кирилл Савицкий как-то рассказал в газете «Ведомости», что однажды его сотрудники нашли на свалке в одном городе целую сумку старых финансовых документов местного завода, активами которого как раз интересовалась компания. Даже из бумаг 10—15-летней давности можно узнать много интересного, например, о наличии у завода побочных бизнесов. Затем проследить их историю, найти несколько нарушений законодательства при приватизации и продаже этих предприятий и, купив несколько акций приглянувшегося завода, оспорить в суде старые сделки по давно

несуществующим «дочкам». Сам Савицкий именно так объяснил сценарий возможной атаки. Однако он не рассказал, как именно использовал «Вашъ финансовый попечитель» бумаги со свалки. И поверьте, таких примеров немало. Так что уничтожать ненужные документы в конце каждого рабочего дня надо обязательно.

Кстати, на Западе изучение мусора конкурента запрещено. Например, в 2001 г. компания Uniliver обвинила Procter Gamble в том, что ее детективы собирали содержимое мусорных баков Uniliver. По итогам переговоров, занявших полтора года, стороны заключили мировое соглашение, обошедшееся Procter Gamble, по оценкам экспертов, в десятки миллионов долларов. Похожие обвинения в 1991 г. выдвигал производитель косметики Avon против Mary Kay Cosmetics, а в 2000 г. — Microsoft против Oracle. Но Россия-матушка пока до таких тонкостей не дошла. Поэтому раздолбаи-сотрудники хоть и не ведают, что творят, но творят... на благо противника.

Зная это, следует уделять отбору, контролю и воспитанию сотрудников большое внимание. Биографии особо важных сотрудников изучать более тщательно. Следует также обращать пристальное внимание как на вновь пришедших на работу, так и на тех, кто подлежит увольнению. Эти люди находятся в ситуациях, наиболее благоприятных для утечки информации. Словом, с людьми надо работать. И если с ними не будет работать ваш клиент и его помощники, то с ними будут работать ваши недоброжелатели. Как гласит армейская поговорка: «Солдат без работы — потенциальный нарушитель».

## 2.2. Вещественно-материальный канал утечки информации

Когда мы говорим о вещественно-материальном канале, то подразумеваем, что информация утекает посредством материальных носителей. Таковыми являются: документы, фотографии, электронные носители, газеты и журналы, дайджесты, аналитические обзоры, видеозаписи, продукция, отходы и т. д.

Как это ни покажется странным, но основной объем информации разведчики получают из открытых источников. Александр Савельев, пресс-секретарь группы «Сигма», пару лет назад признавался, что 90% данных об объекте поглощения его компания добывает из СМИ и Интернета. Особенно полезна бывает региональная пресса. Например, по его утверждению, они долго не могли выяснить, кто такая Юлия Конкина, владеющая 9% акций сотового оператора СМАРТ. («Сигма» пыталась на тот момент поглотить эту компанию.) О том, что она дочка основного владельца компании Геннадия Кирюшина, они узнали в итоге из одной самарской газеты. Так что про-

тивник внимательно читает и заводские многотиражки, и корпоративную периодику.

Крупные компании отслеживают состояние конкурентов и через информацию, поступающую от государственных органов: статистические и регистрационные данные, налоговую отчетность, сообщения о существенных фактах акционерных обществ. А также приобретают информационные базы с данными по объектам промышленного производства или внешнеэкономической деятельности предприятий. Кроме того, на черном рынке легко можно купить базы данных, причем начиная от информации ГИБДД и заканчивая данными по банковским проводкам, или доходам частных лиц.

Но даже из официальных сообщений компаний хорошие аналитики способны вытащить очень ценную информацию. Например, в тех же «Ведомостях», топ-менеджер крупного кондитерского холдинга рассказывал, как из сообщения о растаможке американской корпорацией Mars производственного оборудования он узнал о планах компании начать в России производство шоколадных конфет и даже смог вычислить время его запуска и мощность. Урон от несвоевременного раскрытия информации превышает все плюсы, которые компании планируют заработать. Очень часто на рынке можно урвать кусок только тогда, когда остальные на него по тем или иным причинам не обратили внимания. Но стоит только конкурентам понять, куда двигается ваша компания, — все ринутся туда же. И у вашего подопечного либо ничего не получится, либо прибыль будет в разы меньше, чем планировалась. А такое состояние дел запросто может привести к банкротству. Особенно если затраты на секретную акцию превышают прибыль, полученную после разглашения информации.

Возможным способом получения вещественно-материальной информации является и использование людей, того же персонала, например. В этом варианте мы фактически видим единение двух каналов утечки информации. Каким образом происходит утечка, мы рассмотрели выше, другой вопрос, что в первом случае носитель информации сам человек, а во втором — те же документы.

К другим способам получения информации по этому каналу относятся: кража, перехват носителей информации на каналах их транспортировки (почта, курьеры), сбор мусора, незаконное копирование данных и т. д. При этом не стоит забывать, что вещественно-материальные носители не всегда являются объектом изучения. Достаточно часто, чтобы серьезно помешать конкуренту, достаточно уничтожить данный носитель. А это можно сделать и прямо в вашем офисе, отправив важный документ в машину для измельчения бумаги.

## 2.3. Технические каналы утечки информации

Под техническим каналом утечки информации понимают совокупность объекта разведки (выделенного помещения), технического средства разведки, с помощью которого перехватывается информация, и физической среды, в которой распространяется информационный сигнал. Вот такая умная научная формулировка.

В зависимости от физической природы возникновения информационных сигналов и среды их распространения технические каналы утечки информации можно разделить на:

- прямые акустические (воздушные) каналы;
- виброакустические (вибрационные) каналы;
- акустооптические (лазерные) каналы;
- акустоэлектрические каналы;
- акустоэлектромагнитные (параметрические) каналы.

Чтобы вникнуть в суть процесса утечки информации по техническим каналам, нам придется окунуться в мир технической терминологии, которая в ряде случаев интересна «технарю» и скучна для «гуманитария». Но что поделаешь, разобраться в них надо. Утешайте себя тем, что в дальнейшем это убережет вас от многих ошибок.

### 2.3.1. Прямые акустические технические каналы утечки информации

В прямых акустических (воздушных) технических каналах утечки информации средой распространения акустических сигналов является воздух. В качестве датчиков средств разведки используются высокочувствительные микрофоны, преобразующие акустический сигнал в электрический (рис. 1).

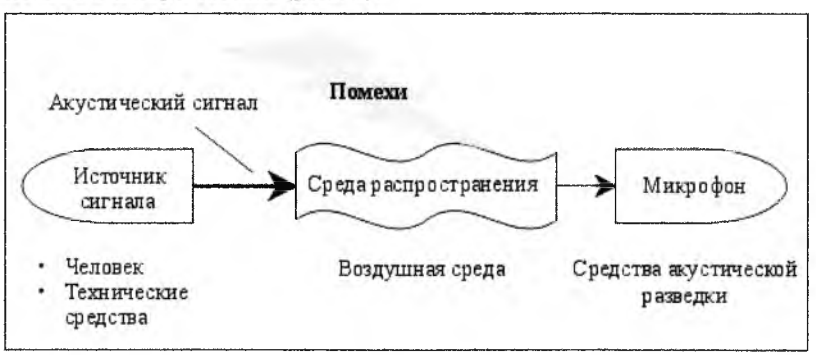



*Рис. 1.*
*Схема прямого акустического технического канала утечки информации*

Перехват акустической (речевой) информации из интересующих помещений по данному каналу может осуществляться:

— с использованием портативных устройств звукозаписи, скрытно установленных в выделенном помещении;
— с использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа (преобразователями акустических сигналов, распространяющихся в воздушной среде), скрытно установленных в помещении, с передачей информации по радиоканалу, оптическому каналу, электросети 220 В, телефонной линии, соединительным линиям ВТСС и специально проложенным кабелям;
— с использованием направленных микрофонов, размещенных в близлежащих строениях и транспортных средствах, находящихся за границей контролируемой зоны;
— без применения технических средств (из-за недостаточной звукоизоляции ограждающих конструкций выделенных помещений и их инженерно-технических систем) посторонними лицами (посетителями, техническим персоналом), при их нахождении в коридорах и смежных помещениях ***(непреднамеренное прослушивание)***.

Использование тех или иных технических средств определяется возможностью доступа в контролируемое помещение посторонних лиц.

В том случае, если имеется постоянный неконтролируемый доступ в интересующее помещение (например, в комнату переговоров), в нем заранее могут быть установлены миниатюрные микрофоны, соединительные линии которых выводятся в специальные помещения, где устанавливается регистрирующая или передающая аппаратура. Причем длина соединительного кабеля может достигать 5000 м. Такие системы перехвата информации часто называют проводными системами (рис. 2).

Чтобы микрофоны не были обнаружены, они выпускаются в сверхминиатюрном исполнении (диаметр менее 2,5 мм) и камуфлируются под предметы интерьера помещений. Современные технологии позволяют изготавливать субминиатюрные микрофоны, которые легко установить за занавеской, в оконной раме или в раме картины.

Для повышения качества перехваченных разговоров микрофоны устанавливаются, как правило, вблизи мест возможного ведения разговоров, например, стола в комнате для ведения переговоров или кафедры в конференц-зале.

Регистрирующая или передающая аппаратура устанавливается, как правило, в местах, доступ в которые затруднен. В качестве регистрирующей аппаратуры используются, как правило, цифровые ре-

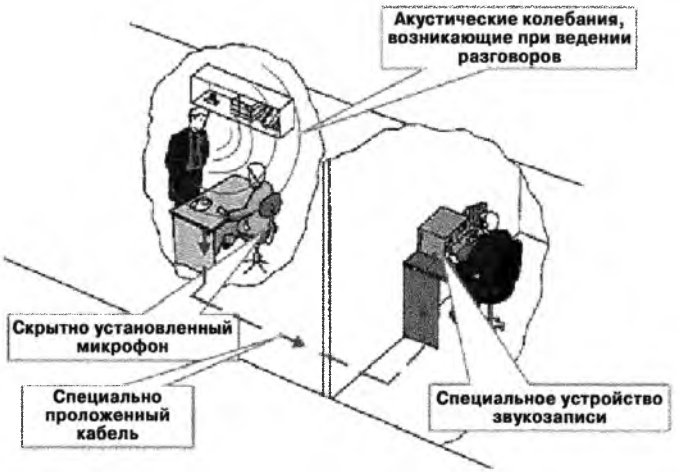



*Рис. 2.*
*Перехват речевой информации с использованием проводной микрофонной системы*

кордеры (магнитофоны) с длительным временем непрерывной записи (от 60 до 300 часов и более).

Для повышения качества и обеспечения возможности коррекции записанного разговора используются стереомагнитофоны и эквалайзеры.

При использовании стереомагнитофонов появляется возможность за счет стереоэффекта дифференцировать и отделять от информативной разговорной речи такие помехи, как шумы бытовых приборов, внешние уличные шумы и т. д.

Эквалайзеры представляют собой специальные устройства с набором различных фильтров: фильтров верхних и нижних частот, полосовых, октавных, чебышевских и других фильтров. Эти фильтры включаются по определенной программе в зависимости от характера искажений сигнала и помех.

Наряду с эквалайзерами для повышения разборчивости речи используются специальные программно-аппаратные комплексы, в состав которых входят:

- устройства ввода/вывода речевых сигналов, включающие аналого-цифровой и цифро-аналоговый преобразователи;
- блоки специализированного сигнального процессора, предназначенные для реализации в реальном масштабе времени процедур цифровой обработки речевых сигналов, в частности шумоподавления;

— компьютер со специальным программным обеспечением и другие средства.

При этом устраняются следующие типы искажений: шумы транспортных средств, сетевые наводки, типовые помехи телефонной сети и радиоканалов, плавная музыка, шумы бытовой техники (шум вентилятора, пылесоса, холодильника и т. п.), широкополосные и медленно меняющиеся шумы, компенсация неравномерности АЧХ диктофона и т. п.

Помещения оборудуются системой прослушивания микрофонного типа в основном при строительстве или реконструкции объекта.

Если посторонние лица не имеют постоянного доступа в нужное помещение, но имеется возможность его регулярного кратковременного посещения под различными предлогами (например, для проверки системы освещения, кондиционирования или уборки помещения), то для перехвата речевой информации могут использоваться портативные устройства звукозаписи (в основном цифровые диктофоны), которые скрытно устанавливаются в интерьерах помещений, как правило, непосредственно перед проведением закрытого мероприятия (рис. 3). После окончания мероприятия диктофон из помещения изымается. Такие устройства также могут камуфлироваться под предметы повседневного обихода, например книги, письменные приборы, пачки сигарет и т. д.

В настоящее время зарубежными и отечественными фирмами выпускается огромное количество портативных цифровых диктофонов, которые очень легко спрятать практически в любом помещении. Современные портативные цифровые диктофоны имеют миниатюрные размеры (объем менее 2 — 3 см) и вес (6 — 20 граммов), оборудуются встроенными и миниатюрными выносными микрофонами, имеют устройство управления включения записи голосом (VAS), позволяют фиксировать время, длительность разговора и т. д. Длительность непрерывной записи в цифровых диктофонах в основном определяется емкостью, а следовательно, и размерами аккумуляторной батареи. Например, диктофон Edic-mini B5 — при размерах диктофона 24 × 44 × 8 мм — обеспечивает время непрерывной записи до 17 ч, а диктофон Edic-mini B2 при размерах 18 × 55 мм — до 200 ч.

Недостатком способа перехвата речевой информации с использованием портативных диктофонов является необходимость повторного проникновения в выделенное помещение с целью изъятия диктофона и прослушивания записанных разговоров. Но стоит отметить тот факт, что, поскольку цифровые диктофоны могут быть встроены в авторучку, наручные часы, брелок и т. п., в ряде случаев (информацию собирает партнер по бизнесу, секретарь, любое дру-

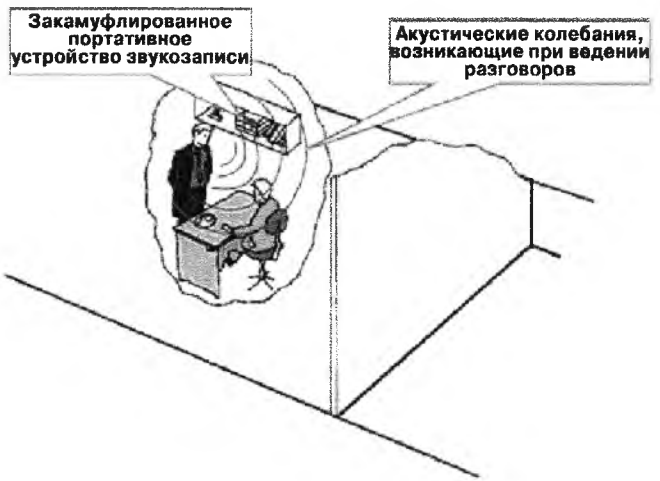



*Рис. 3.*
*Перехват речевой информации с использованием портативных устройств звукозаписи с датчиками микрофонного типа, скрытно установленных в выделенном помещении*

гое лицо, присутствующее при переговорах) нет необходимости оставлять диктофон в помещении заранее. Достаточно будет принести его с собой и унести по окончании переговоров. Но если лицо, занимающееся сбором информации, не имеет возможности попасть на них, то придется делать закладку заранее и впоследствии забирать ее. Способ накладный, причем главным образом из-за времени. Информация бывает настолько «горячей», что воспользоваться ей через несколько часов уже будет невозможно. Как ни крути, а это очень существенный недостаток.

Такого недостатка лишены электронные устройства перехвата информации (закладные устройства).

Под закладными устройствами обычно понимают портативные устройства съема информации, скрытно внедряемые (закладываемые) в выделенные помещения, в том числе в ограждающие конструкции, оборудование, предметы интерьера, а также в технические средства и системы обработки информации, вспомогательные технические средства и системы и передающие перехваченную информацию на приемный пункт по различным каналам.

Закладные устройства можно классифицировать по типу используемых датчиков, виду исполнения, типу источника питания, способам передачи информации и ее кодирования, способу управления передатчиком, месту установки и т. д. (табл. 1).

*Таблица 1*

**Классификация электронных устройств перехвата речевой информации (закладных устройств)**

| № п/п | Наименование показателей классификации | Значение показателей классификации |
|---|---|---|
| 1. | Вид датчика | Микрофонный<br>Контактного типа (вибродатчик) |
| 2. | Вид исполнения | Обычные (отдельные модули)<br>Камуфлированные |
| 3. | Место установки | В предметах интерьера<br>В конструкциях здания<br>В электро-, радиоприборах и электросети 220 В<br>В телефонных аппаратах, ВТСС и их соединительных линиях |
| 4. | Способ передачи информации | По радиоканалу (радиозакладки)<br>По оптическому каналу в инфракрасном диапазоне (ИК-закладки)<br>По сети электропитания 220 В (сетевые закладки)<br>По телефонной линии (закладки типа «телефонное ухо») |
| 5. | Вид используемых сигналов | С простыми сигналами (AM-, NFM-, WFM-модуляция)<br>Со сложными сигналами (шумоподобные с псевдослучайной фазовой модуляцией (М-последовательность, код Рида – Мюллера и т. п.)<br>С псевдослучайной перестройкой несущей частоты (ППРЧ) и т. д.) |
| 6. | Тип источника питания | От аккумуляторов<br>От электросети 220 В<br>От телефонной линии<br>От внешнего источника радиоизлучения |
| 7. | Способ управления включением передатчика | Неуправляемые<br>С системой типа VOX (акустопуском)<br>Дистанционно управляемые |
| 8. | Способ накопления информации | Без накопления<br>С промежуточным накоплением (с коротким и длительным временем накопления) |
| 9. | Способ кодирования информации | Без кодирования информации<br>С аналоговым скремблированием сигнала<br>С цифровым шифрованием информации |
| 10. | Используемый диапазон длин волн | LF (НЧ)-диапазон (километровые волны)<br>MF (СЧ)-диапазон (гектометровые волны)<br>HF (ВЧ)-диапазон (декаметровые волны)<br>VHF (ОВЧ)-диапазон (метровые волны)<br>UHF (УВЧ)-диапазон (дециметровые волны)<br>SHF (ОНг)-ГГц диапазон (сантиметровые волны) |

Закладные устройства перехвата речевой информации с датчиками микрофонного типа часто называют акустическими закладками. Они могут быть выполнены в виде отдельного модуля, как правило, в форме параллелепипеда, или закамуфлированы под предметы повседневного обихода: пепельницу, электронный калькулятор, электролампочку, зажигалку, наручные часы, авторучку, вазу и т. п.

Питание акустических закладок осуществляется от автономных источников питания (аккумуляторов, батарей), электросети переменного тока или телефонной сети. В зависимости от мощности излучения и типа источника питания время работы акустической закладки составляет от нескольких часов до нескольких суток и даже месяцев. При электропитании от сети переменного тока или телефонной линии время их работы не ограничено.

Перехватываемая акустическими закладками информация может или записываться с использованием портативных устройств звукозаписи, или передаваться к внешним средствам регистрации по радио- и оптическому каналам, электросети переменного тока, телефонным линиям и т. д. В качестве внешних устройств регистрации речевой информации наиболее широко используются цифровые диктофоны и ПК, устанавливаемые в местах сбора разведывательной информации.

Акустические закладки, передающие информацию по радиоканалу, представляют собой специальные миниатюрные радиопередатчики и часто называются радиозакладками (рис. 4).

Для передачи информации используются VHF (метровый), UHF (дециметровый) и GHz (ГГц) диапазоны длин волн. Наиболее часто используются диапазоны частот: 130 — 174 МГц; 350 — 450 МГц; 850 — 950 МГц и 1100 — 1300 МГц. Однако не исключено использование и других поддиапазонов (см. приложение 3). Например, радиозакладка SIM-A-31T работает в диапазоне 10,5 ГГц.

Дальность передачи информации во многом зависит от мощности излучения и вида используемой модуляции. Как правило, без использования ретрансляторов дальность передачи не превышает 300 — 500 м.

Современные радиозакладки оборудуются системой дистанционного управления, которое используется для включения и выключения передатчика. Использование системы дистанционного управления значительно повышает скрытность ее использования, а также увеличивает время работы.

Недостатком радиозакладок является возможность обнаружения их радиоизлучений специальными приемниками. С целью устранения этого недостатка разработаны закладные устройства, передающие информацию по оптическому каналу в инфракрасном,


*Рис. 4.*
*Перехват речевой информации с использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа, скрытно установленных в выделенном помещении, с передачей информации по радиоканалу (радиозакладками)*

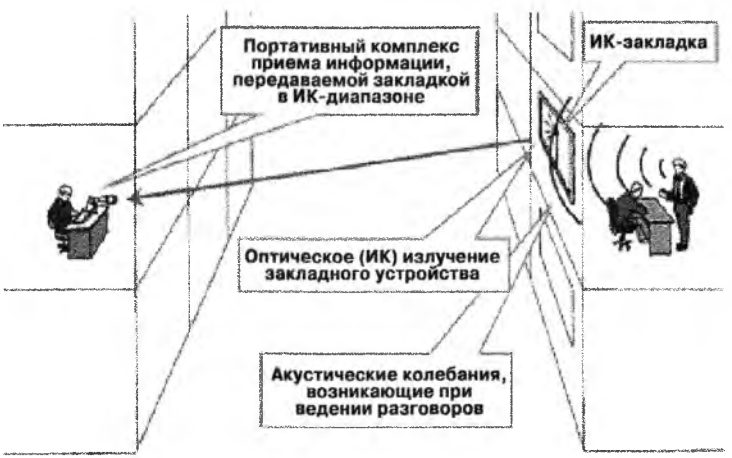



*Рис. 5.*
*Перехват речевой информации с использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа, скрытно установленных в выделенном помещении, с передачей информации по оптическому каналу в инфракрасном диапазоне длин волн (ИК-закладками)*

не видимом глазу диапазоне (0,8 — 1,1 мкм). Такие закладки иногда называют «инфракрасными» или ИК-закладками (рис. 5). Инфракрасный передатчик преобразует акустические колебания в световые, используя при этом широтно-импульсную модуляцию. Для приема информации, передаваемой такими закладками, используются приемники оптического излучения. Дальность передачи информации составляет несколько сот метров.

Кроме радио и оптического канала, для передачи информации используются линии электропитания силовой сети 220 В (рис. 6). Такие закладки часто называют сетевыми. Они могут быть установлены в электрические розетки, удлинители, бытовую аппаратуру, питающуюся от сети переменного тока, или непосредственно в силовую линию. Для приема информации, передаваемой сетевыми закладками, используются специальные приемники, подключаемые к силовой сети в пределах здания (силовой подстанции).

Принцип работы сетевой закладки мало чем отличается от принципа работы обычной радиозакладки, у которой в качестве антенны используется силовой провод, но при этом в основном используют частоты от 40 до 600 кГц (в ряде случаев могут использоваться частоты до 5 — 10 МГц).

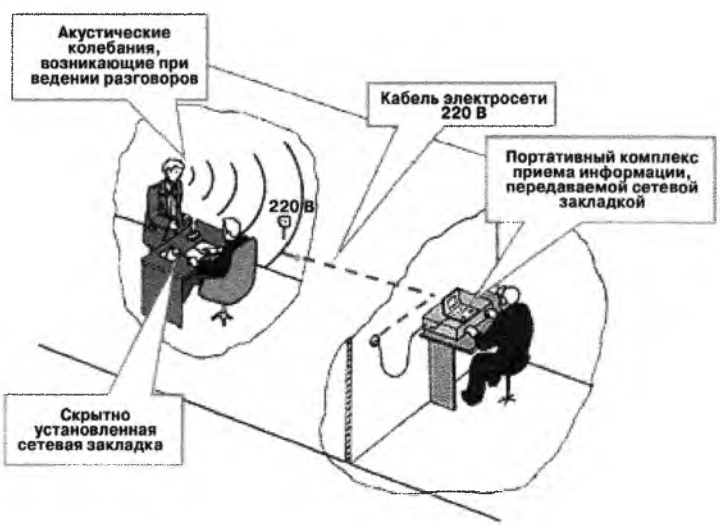



*Рис. 6.*
*Перехват речевой информации с использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа, скрытно установленных в выделенном помещении, с передачей информации по электросети 220 В (сетевыми закладками)*

С использованием сетевых закладок возможна передача информации на расстояния до 300 — 500 м в пределах одного или нескольких зданий, питающихся от одной низковольтной шины трансформаторной подстанции.

Кроме сети электропитания, для передачи информации широко используются телефонные линии связи. Наибольшее распространение среди таких закладок нашли устройства типа «телефонного уха», прием информации с которых может осуществляться с обычного или сотового телефона (рис. 7). Данное устройство включает в себя контроллер состояния телефонной линии, дешифратор, электронный коммутатор, микрофонный усилитель и непосредственно микрофон, устанавливаемый в контролируемом помещении. Устройство включается в разрыв телефонной линии, соединенной с телефоном, номер которого известен («телефоном-наблюдателем»).

К одному устройству контроля может подключаться более пяти микрофонов.

Дальность передачи при использовании такой закладки практически не ограничена, так как вызов можно осуществлять по международным каналам телефонной связи. Питание устройства осуществляется от телефонной линии, поэтому срок службы такой закладки практически не ограничен.

Способы внедрения закладных устройств во многом зависят от режима доступа в служебные помещения.

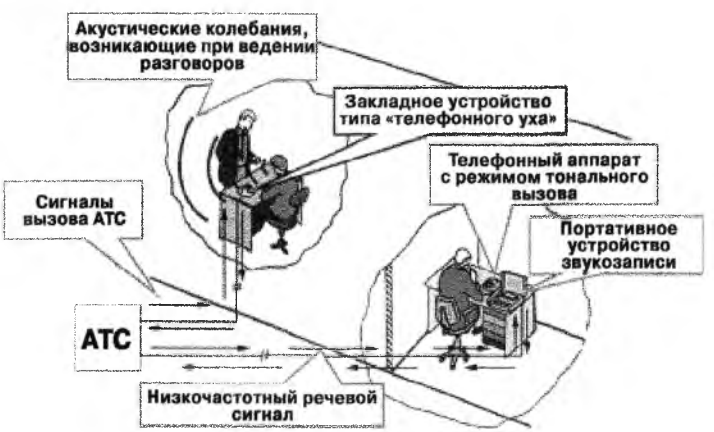



*Рис. 7.*

*Перехват речевой информации с использованием электронных устройств перехвата информации (закладных устройств) с датчиками микрофонного типа, скрытно установленных в выделенном помещении, с передачей информации по телефонной линии на низкой частоте (закладки типа «телефонное ухо»)*

Если доступ в помещение не контролируется, то закладные устройства могут быть установлены в интерьерах помещения, предметах повседневного обихода, радиоаппаратуре, розетках электросети и электрических приборах, технических средствах связи и их соединительных линиях и т. п. Наиболее вероятна установка закладок при профилактических работах на системах электропитания, связи и сигнализации или уборке помещений.

Если доступ в помещение контролируется, но там даже в течение короткого времени могут находиться посетители (чаще всего это кабинеты, приемные или комнаты отдыха руководящего состава), то закладки могут быть установлены или путем замены предметов, постоянно находящихся в данном помещении, на аналогичные, но оборудованные закладками, или непосредственно в интерьерах помещения, например под креслом или столом, под подоконником, за занавеской и т. п., или даже в смятой пачке сигарет или куске картона, брошенных в урну.

Закладки могут быть закамуфлированы в предметах и вещах, «случайно» забытых посетителем, например, в авторучке, калькуляторе, кейсе, шляпе и т. д. Закладки могут быть установлены в сувенирах или предметах повседневного обихода, подаренных руководителю, в средствах иностранного производства, поставляемых по предварительным заказам предприятий и учреждений. Они также могут быть установлены в импортную и отечественную аппаратуру при ее гарантийном обслуживании или ремонте.

Если требуется организовать прослушивание разговоров в помещении, доступ в которое невозможен, то для прослушивания разговоров в помещении могут использоваться направленные микрофоны.

Разведка может вестись из соседних зданий или автомашин, находящихся на автостоянках, прилегающих к зданию.

С использованием направленных микрофонов возможен перехват речевой информации из интересующих противника помещений при наличии открытых оконных проемов (форточек или фрамуг). В условиях города (на фоне транспортных шумов) перехват возможен на расстояниях до 50 — 100 м. За городом при оптимальных условиях дальность разведки может составлять до 100 — 150 м днем и до 500 м в ночное время.

В основном используются три вида направленных микрофонов: параболические (рефлекторные), трубчатые («микрофон-труба») и плоские (микрофонные решетки) микрофоны.

Параболический микрофон имеет параболический отражатель, в фокусе которого находится обычный высокочувствительный микрофон.

Наиболее простым по конструкции является направленный микрофон «Большое ухо», выпускаемый в Германии. Основой устройства является параболоид вращения диаметром 43 см, в фокусе которого помещен электретный микрофон, подключенный ко входу малошумящего усилителя низкой частоты, собранного на четырех операционных усилителях, конструктивно оформленных в одном корпусе интегральной микросхемы.

«Микрофон-труба» представляет собой трубчатую фазированную приемную акустическую антенну, нагруженную на высокочувствительный микрофон или решетку микрофонов, включенных последовательно.

«Микрофон-труба» может быть закамуфлирован под зонт, трость или выполнен в обычном исполнении.

Так называемые «плоские» направленные микрофоны появились сравнительно недавно и представляют собой акустическую антенную решетку, включающую несколько десятков микрофонов. Они могут встраиваться в стенку атташе-кейса или вообще носиться в виде жилета под рубашкой или пиджаком. Дальность их действия сравнительно ниже по отношению к первым двум типам направленных микрофонов и составляет 30 — 50 м.

### 2.3.2. Виброакустические и акустооптический (лазерный) технические каналы утечки информации

В виброакустических (вибрационных) технических каналах утечки информации акустические сигналы, возникающие при ведении разговоров в выделенном помещении, при воздействии на строительные конструкции (стены, потолки, полы, двери, оконные рамы и т. п.) и инженерно-технические коммуникации (трубы водоснабжения, отопления, канализации, воздуховоды и т. п.) вызывают в них упругие (вибрационные) колебания, которые и регистрируются датчиками средства разведки (рис. 8).

Для перехвата речевой информации по виброакустическим каналам в качестве средств акустической разведки используются электронные стетоскопы и закладные устройства с датчиками контактного типа. Наиболее часто для передачи информации с таких закладных устройств используется радиоканал, поэтому их называют радиостетоскопами.

В качестве датчиков средств акустической разведки используются контактные микрофоны (вибропреобразователи), чувствительность которых составляет от 50 до 100 мкВ/Па, что дает возможность прослушивать разговоры и улавливать слабые звуковые колебания (шорохи, тиканье часов и т. д.) через бетонные и кирпичные

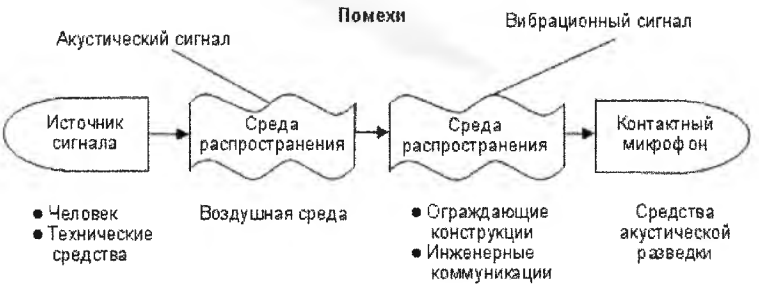



*Рис. 8.*
*Схема виброакустического технического канала утечки информации*

стены толщиной более 100 см, а также двери, оконные рамы и инженерные коммуникации.

Электронные стетоскопы и закладные устройства с датчиками контактного типа позволяют перехватывать речевую информацию без физического доступа «агентов» в помещения. Их датчики наиболее часто устанавливаются на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

При этом возможности по перехвату информации будут во многом определяться затуханием информационного сигнала в ограждающих конструкциях и уровнем внешних шумов в месте установки контактного микрофона (табл. 2, 3).

*Таблица 2*

**Затухание вибрационных сигналов на ограждающих конструкциях**

| Наименование конструкции | Затухание сигнала, дБ |
|---|---|
| Стена в 0,5 кирпича | 40 – 48 |
| Стена в 1 кирпич | 44 – 53 |
| Стена в 2 кирпича | 46 – 60 |
| Стена из железобетонных блоков (100 мм) | 40 – 50 |
| Стена из железобетонных блоков (200 мм) | 44 – 60 |
| Окно одинарное (4 мм) | 22 – 28 |
| Окно двойное (4 мм) | 32 – 48 |
| Дверь типовая | 23 – 34 |
| Дверь металлическая, облицованная | 32 – 48 |

*Таблица 3*

**Средний интегральный уровень вибрационных шумов**

| Наименование конструкции | Уровень шума, дБ |
|---|---|
| Внешняя конструкция здания | 15 – 35 |
| Внутренняя конструкция здания | 10 – 30 |
| Внешнее стекло окна | 25 – 30 |
| Внутреннее стекло окна | 10 – 15 |
| Трубопровод отопления с водой | 10 – 15 |
| Трубопровод отопления без воды | 10 – 20 |

Проведенные измерения и расчеты показали, что качество добываемой средствами акустической разведки речевой информации по прямому акустическому и виброакустическому каналам вполне достаточно для составления подробной справки о содержании перехваченного разговора (табл. 4).

*Таблица 4*

**Разборчивость речи при перехвате информации средствами разведки по прямому акустическому и виброакустическому каналам**

| Место установки датчика аппаратуры акустической разведки | Вид принимаемого сигнала | Словесная разборчивость, % |
|---|---|---|
| За окном на расстоянии 1,0 – 1,5 м от оконной рамы при закрытой форточке | Прямой акустический | 67 – 80 |
| За окном на расстоянии 1,0 – 1,5 м от оконной рамы при открытой форточке | Прямой акустический | 97 – 98 |
| На оконной раме или внешнем оконном стекле при закрытой форточке | Виброакустический | 71 – 80 |
| За дверью (без тамбура) | Прямой акустический | 91 – 97 |
| За перегородкой из материалов типа гипсолит, асбестоцемент | Прямой акустический | 71 – 87 |
| На перегородке из материалов типа гипсолит, асбестоцемент | Виброакустический | 84 – 95 |
| На железобетонной стене | Виброакустический | 80 – 98 |
| В воздуховоде (6 – 8 м от ввода) | Прямой акустический | 87 – 95 |
| На трубопроводе (через этаж) | Виброакустический | 95 – 97 |

Электронные стетоскопы, как правило, устанавливаются в смежных (служебных и технических) помещениях (рис. 9), а радиостетоскопы, ввиду своей миниатюрности, — в малозаметных местах на наружных поверхностях зданий, на оконных проемах и рамах (рис. 10), за дверными проемами, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

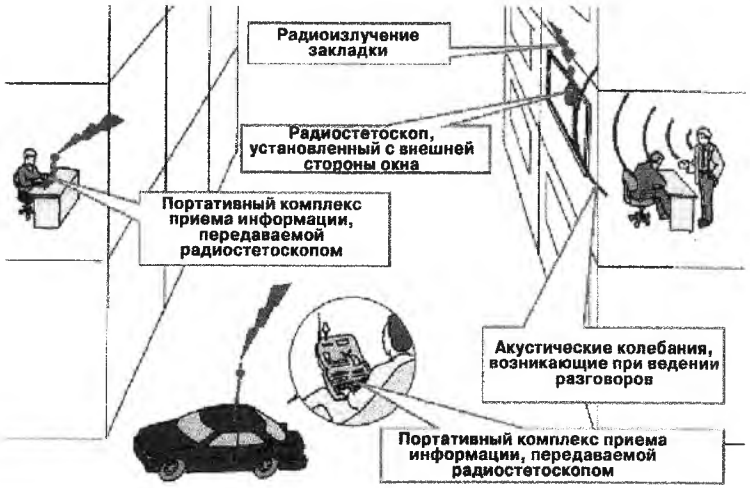



*Рис. 9.*
*Перехват речевой информации с использованием электронных стетоскопов из смежных помещений, принадлежащих другим организациям (учреждениям) и расположенных в том же здании, что и выделенные помещения*

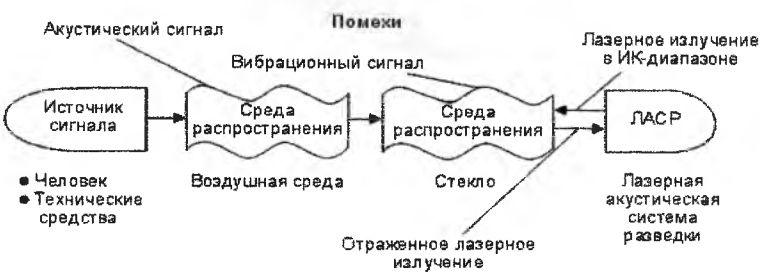



*Рис. 10.*
*Перехват речевой информации с использованием закладных устройств с датчиками контактного типа, скрытно установленных с внешней стороны окна, с передачей информации по радиоканалу (радиостетоскопами)*

Для установки на внешних оконных стеклах могут использоваться сверхминиатюрные радиостетоскопы, покрытые липкой резиновой массой и по внешнему виду напоминающие шарик или комочек грязи. Такой шарик путем ручного броска приклеивается с наружной стороны окна и передает информацию в течение 1—2 дней, по их истечении резиновая масса высыхает, закладка отлипает от поверхности, на которой была прикреплена, и падает.

Для установки радиостетоскопов в местах, физический доступ к которым невозможен, используются специальные бесшумные пистолеты или арбалеты, стреляющие «стрелами — радиозакладками». Стрела с миниатюрной радиозакладкой, в ударостойчивом исполнении, надежно прикрепляется к поверхностям из любого материала: металла, дерева, пластмассы, стекла, камня, бетона и т. п. при выстреле с расстояния до 25 м.

В период строительства в стены здания могут быть встроены радиостетоскопы длительного времени действия, оснащенные системой дистанционного управления. Время работы таких устройств может составлять в режиме дежурного приема более 10 лет, а в режиме передачи — более 6 месяцев. Наиболее часто такие устройства камуфлируются под обычные кирпичи. Датчики акселерометрического типа такого «кирпича» перехватывают вибрационные колебания, возникающие при ведении разговоров в помещениях, в диапазоне частот от 100 Гц до 10 кГц. Дальность передачи информации с таких устройств в UHF-диапазоне обычно составляет 300 — 500 м.

Акустооптический (лазерный) технический канал утечки информации образуется при облучении лазерным лучом вибрирующих в акустическом поле, возникающем при ведении разговоров, тонких отражающих поверхностей (стекол окон, картин, зеркал и т. д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация (рис. 11). Причем лазер и приемник оптического излучения могут быть установлены в одном или разных местах (помещениях) (рис. 12).

Для перехвата речевой информации по данному каналу используются сложные лазерные акустические системы разведки (ЛАСР), иногда называемые «лазерными микрофонами».

ЛАСР состоит из источника когерентного излучения (лазера) и приемника оптического излучения, оснащенного фокусирующей оптикой. Для обеспечения высокой механической устойчивости передатчика и приемника, что крайне необходимо для нормальной работы системы, последние устанавливаются на треножных штативах. Передатчик и приемник переносятся в обычном портфеле-дипломате. Как правило, в таких системах используются лазеры, работающие в не видимом глазу ближнем инфракрасном диапазоне длин волн (0,75 — 1,1 мкм).

Принцип действия системы заключается в следующем. Передатчик осуществляет облучение наружного оконного стекла узким ла-

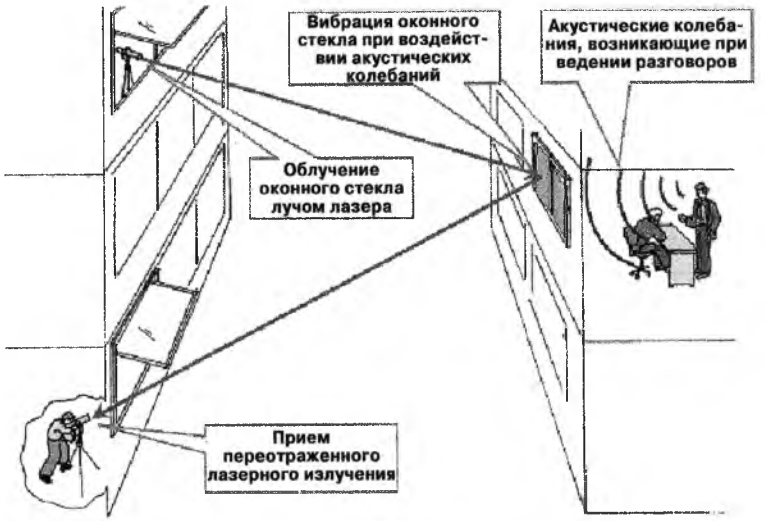



*Рис. 11.*
*Схема акустического (лазерного) технического канала утечки информации*

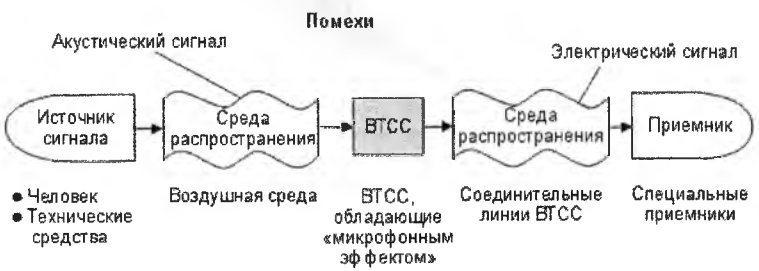



*Рис. 12.*
*Перехват речевой информации с использованием лазерной акустической системы разведки путем «лазерного зондирования» оконных стекол*

зерным лучом. Приемник принимает рассеянное отраженное излучение, модулированное по амплитуде и фазе по закону изменения акустического (речевого) сигнала, возникающего при ведении разговоров в контролируемом помещении. Принятый сигнал детектируется, усиливается и прослушивается на головных телефонах или записывается на магнитофон. Для улучшения разборчивости речи в приемнике используется специальное шумоподавляющее устройство.

Данные системы наиболее эффективны для прослушивания разговоров в помещениях небольшого размера, которые по своим акустическим характеристикам близки к объемному резонатору, когда все двери и окна помещения достаточно хорошо герметизированы. Эффективны они и для подслушивания разговоров, ведущихся в салонах автомашин.

Современные ЛАСР позволяют «снимать» информацию не только с наружных, но и внутренних оконных стекол, зеркал, стеклянных дверей и других предметов. Для увеличения дальности разведки оконные стекла обрабатывают специальным составом, значительно увеличивающим коэффициент отражения лазерного излучения, или устанавливают на них специальные направленные отражатели (триппель-призмы).

Лазерные акустические системы разведки имеют дальность действия при приеме диффузно отраженного излучения до 100 м, при обработке (покрытии) стекол специальным материалом — более 300 м, а при установке на оконных стеклах триппель-призм — более 500 м.

### 2.3.3. Акустоэлектрические и акустоэлектромагнитные (параметрические) технические каналы утечки информации

Акустоэлектрические технические каналы утечки информации возникают вследствие преобразования информативного сигнала из акустического в электрический за счет «микрофонного» эффекта в электрических элементах вспомогательных технических средств и систем (ВТСС).

Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов, дроссели ламп дневного света, электрореле и т. п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником акустических колебаний. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), изменяющейся по закону воздействующего информационного акустического поля, либо к модуляции токов, протекающих по этим элементам, информационным сигналом. Например, акустическое поле, воздействуя на якорь электромагнита вызывного телефонного звонка, вызывает его колебание. В результате чего изменяется магнитный поток сердечника электромагнита. Изменение этого потока вызывает появление ЭДС самоиндукции в катушке звонка, изменяющейся по закону изменения акустического поля.

ВТСС, кроме указанных элементов, могут содержать непосредственно электроакустические преобразователи. К таким ВТСС относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект электроакустического преобразования акустических колебаний в электрические часто называют «микрофонным эффектом». Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного (гальванического) подключения к соединительным линиям ВТСС, обладающим «микрофонным эффектом», специальных высокочувствительных низкочастотных усилителей (пассивный акустоэлектрический канал) (рис. 13). Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты (рис. 14). Но вследствие незначительного уровня наведенной ЭДС дальность перехвата речевой информации, как правило, не превышает нескольких десятков метров.

Активный акустоэлектрический технический канал утечки информации образуется путем несанкционированного контактного введения токов высокой частоты от соответствующего генератора в линии (цепи), имеющие функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным (рис. 15). Информационный сигнал в данных элементах ВТСС появляется

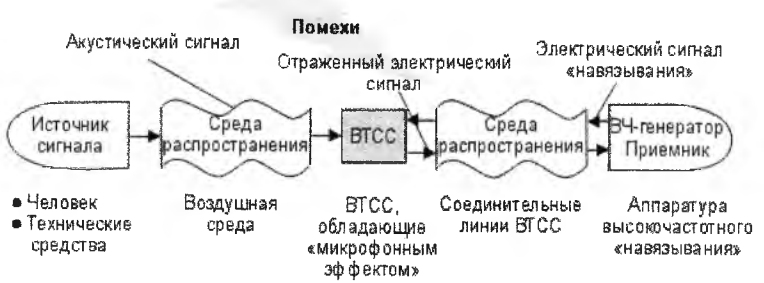



*Рис. 13.*
*Схема акустоэлектрического пассивного технического канала утечки информации*

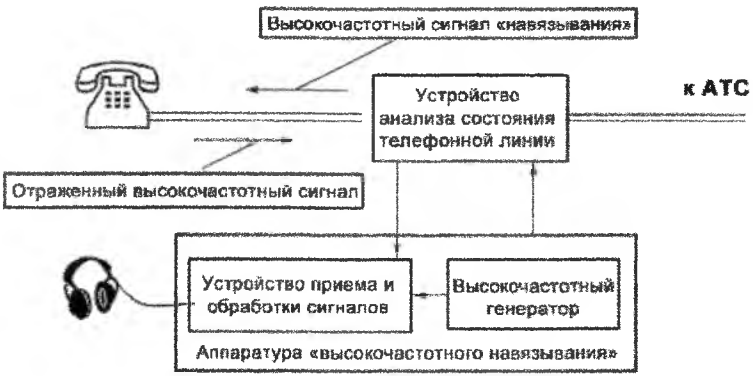



*Рис. 14.*
*Перехват речевой информации путем подключения специальных низкочастотных усилителей к соединительным линиям ВТСС, обладающих «микрофонным эффектом»*

вследствие электроакустического преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используются специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы.

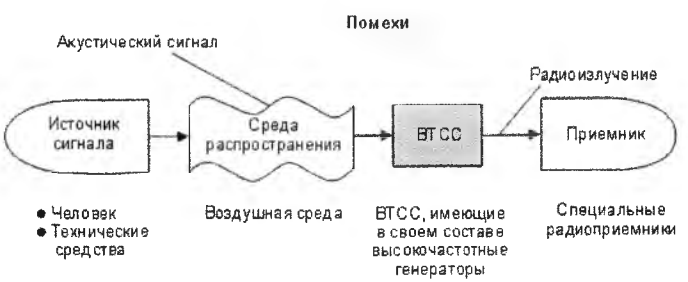



*Рис. 15.*
*Схема акустоэлектрического активного технического канала утечки информации*

Такой метод получения информации часто называется методом «высокочастотного навязывания» и в основном используется для перехвата разговоров, ведущихся в помещении, путем подключения к линии телефонного аппарата, установленного в контролируемом помещении (рис. 16). Для исключения воздействия высокочастотного сигнала на аппаратуру АТС в линию, идущую в ее сторону, устанавливается специальный фильтр нижних частот. Аппаратура «высокочастотного навязывания» может подключаться к телефонной линии на удалении до нескольких сот метров от выделенного помещения.

*Акустоэлектромагнитные (параметрические) технические каналы утечки информации можно разделить на пассивные и активные.*

Образование пассивного акустоэлектромагнитного канала утечки информации связано с наличием в составе некоторых ВТСС высокочастотных генераторов. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т. п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а следовательно, к изменению частоты излуче-


*Рис. 16.*
*Перехват речевой информации путем подключения аппаратуры «высокочастотного навязывания» к соединительным линиям ВТСС, обладающих «микрофонным эффектом»*

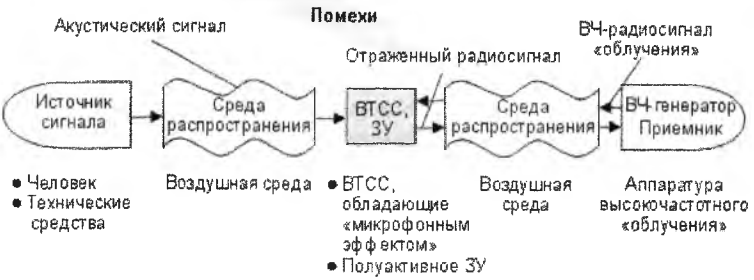



*Рис. 17.*
*Схема акустоэлектромагнитного(параметрического) пассивного технического канала утечки информации*


*Рис. 18.*
*Перехват речевой информации путем приема и детектирования побочных электромагнитных излучений ВТСС, обладающих «микрофонным эффектом» (на частотах работы их высокочастотных генераторов)*

ния генератора, т. е. к частотной модуляции сигнала. Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы

переменной емкости с воздушным диэлектриком в колебательных контурах гетеродинов.

Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств, установленных в выделенном помещении, могут быть перехвачены средствами радиоразведки. Данный акустоэлектромагнитный (параметрический) технический канал утечки информации называется пассивным (рис. 17, 18).

### 2.3.4. Технические каналы утечки информации, передаваемой по каналам связи

На связи хотелось бы остановиться особо. В последнее время это чуть ли не самый главный после персонала источник утечки информации.

**А) Проводные телефоны**

До настоящего времени телефонная связь превалирует среди многих видов электрорадиосвязи, поэтому телефонный канал является основным, на базе которого строятся узкополосные и широкополосные каналы для других видов связи.

Использование тех или иных средств для перехвата информации, передаваемой по телефонным линиям связи, будет определяться возможностью доступа к линии связи.

Перехват информации с обычных абонентских двухпроводных телефонных линий может осуществляться или путем непосредственного контактного подключения к линиям, или с использованием простых малогабаритных индуктивных датчиков, подключаемых к одному из проводов абонентской линии.

Факт контактного подключения к линии связи легко обнаружить. При подключении индукционного датчика целостности оплетки кабеля не нарушается, параметры кабеля не изменяются и обнаружить факт подключения к линии в этом случае практически невозможно.

Информация, перехватываемая с телефонной линии, может записываться на диктофон или передаваться по радиоканалу с использованием микропередатчиков, которые часто называют телефонными закладками или телефонными ретрансляторами.

Телефонные закладки можно классифицировать по виду исполнения, месту установки, источнику питания, способу передачи информации и ее кодирования, способу управления и т. д. (рис. 19).


*Рис. 19.*
*Классификация телефонных закладок*

Выполняются они, как правило, или в виде отдельного модуля, или камуфлируются под элементы телефонного аппарата, например, конденсатор, телефонный или микрофонный капсюли, телефонный штекер, розетку и т. д.

Телефонные закладки в обычном исполнении имеют небольшие размеры (объем от 1 до 6 — 10 см) и вес от 10 до 70 г.

Перехваченную информацию телефонные закладки передают, как правило, по радиоканалу. Обычно в качестве антенны используется телефонный провод.

Дальность передачи информации может составлять от 200 до 600 м.

Передача информации (работа на излучение) начинается в момент поднятия трубки абонентом. Однако встречаются закладки, производящие запись информации в цифровой накопитель и передающие ее по команде.

Телефонные закладки могут быть установлены: в корпусе телефонного аппарата, телефонной трубке или телефонной розетке, а также непосредственно в тракте телефонной линии.

Возможность установки телефонной закладки непосредственно в телефонной линии имеет важное значение, так как для перехвата телефонного разговора нет необходимости проникать в помещение, где находится один из абонентов. Телефонные закладки могут быть установлены или в тракте телефонной линии до распределительной коробки, находящейся, как правило, на одном этаже с помещением, где установлен контролируемый аппарат, или в тракте телефонной

линии от распределительной коробки до распределительного щитка здания, располагаемого обычно на первом этаже или в подвале здания.

Телефонные закладки могут быть установлены последовательно в разрыв одного из телефонных проводов, параллельно или через индуктивный датчик.

Наряду с контактным подключением возможен и бесконтактный съем информации с телефонной линии. Для этих целей используются закладки с миниатюрными индукционными датчиками. Такие закладки питаются от автономных источников питания и установить факт подключения их к линии даже самыми современными средствами практически невозможно, так как параметры линии при подключении не меняются.

При питании от телефонной линии время работы закладки не ограничено. При использовании автономных источников питания время работы закладки составляет от нескольких десятков часов до нескольких недель.

Способы применения телефонных закладок определяются возможностью доступа в помещение, где установлен контролируемый телефонный аппарат.

В случае, если имеется возможность даже на короткое время проникнуть в помещение, закладка может быть установлена в корпусе телефонного аппарата, телефонной трубке и т. д. Причем для этого необходимо от 10 — 15 с до нескольких минут. Например, замена обычного микрофонного капсюля на аналогичный, но с установленной в нем телефонной закладкой занимает не более 10 с. Причем визуально их отличить невозможно.

Телефонные закладки, выполненные в виде отдельных элементов схемы телефонного аппарата, впаиваются в схему вместо аналогичных элементов или маскируются среди них. Наиболее часто используются закладки, выполненные в виде различного типа конденсаторов. Для установки таких устройств требуется несколько минут и проводится установка, как правило, при устранении неисправностей или профилактическом обслуживании телефонного аппарата.

Не исключена возможность установки закладки в телефонный аппарат еще до поступления его в учреждение или на предприятие.

Если доступ в контролируемое помещение невозможен, закладки устанавливаются или непосредственно в тракте телефонной линии, или в распределительных коробках и щитках обычно таким образом, чтобы их визуальное обнаружение было затруднено.

Чем меньше закладка, тем легче ее замаскировать. Однако небольшие по размерам закладки в ряде случаев не обеспечивают тре-

буемой дальности передачи информации. Поэтому для увеличения дальности передачи информации используются специальные ретрансляторы, устанавливаемые, как правило, в труднодоступных местах или в автомашине в радиусе действия закладки.

**Б) Сотовые телефоны («мобильники»)**

Сотовый телефон — одно из величайших изобретений человечества, подарившее человеку свободу общения и передвижения.

Но в то же время мобильник является прекрасным радиомаяком, позволяющим отслеживать любые перемещения абонента в пространстве.

Структура сотовых сетей представляет собой совокупность примыкающих друг к другу и имеющих различные частоты связи небольших зон обслуживания, которые могут охватывать обширные территории. Поскольку радиус одной такой зоны (ячейки, соты) не превышает, как правило, нескольких километров, в сотах, непосредственно не примыкающих друг к другу, возможно повторное использование без взаимных помех одних и тех же частот.

В каждой из ячеек размещается стационарная (базовая) приемопередающая радиостанция, которая связана проводной связью с центральной станцией сети. Число частотных каналов в сети обычно не превышает 7 — 10, причем один из них организационный. Переход абонентов из одной зоны в другую не сопряжен для них с какими-либо перестройками аппаратуры. Когда абонент пересекает границу зоны, ему автоматически предоставляется другая свободная частота, принадлежащая новой ячейке. Основные технические характеристики сотовых систем связи представлены в табл. 5.

Итак, все соты оборудованы собственными вышками или базовыми станциями. И при этом все вышки имеют четкий адрес. В результате в технической информации о конкретном соединении содержится не только телефонный номер абонента, с которым связался владелец «трубки», но и адрес вышки, через которую осуществлялась коммутация. Кроме того, фиксируется и так называемый сектор — то есть информация о том, где находился звонивший относительно вышки (к северу, югу, западу или востоку). К тому же технические возможности аппаратуры сотовых компаний позволяют определить мощность сигнала, что в свою очередь указывает на то, где находился абонент в момент разговора — на улице, в машине или в здании.

**Основные технические характеристики сотовых систем связи**

*Таблица 5*

| Система (стандарт) | Наименование характеристик | | | | |
|---|---|---|---|---|---|
| | Полосы частот, МГц | Ширина полосы частот канала, кГц | Максимальная мощность, Вт | Число каналов | Класс сигналов, тип модуляции |
| NMT-450 | 453–457,5 (ПС)<br>463–467,5 (БС) | 25 | 50 (БС) 15 (ПС) | 180 | 16KOF3EJN |
| AMPS | 825–845 (ПС)<br>870–890 (БС) | 30 | 45(БС) 12 (ПС) | 666 | 30K0F3E |
| D-AMPS | 825–845 (ПС)<br>870–890 (бс) | 30 | – | 832 | 30K0G7WDT / 4 DQPSK |
| GSM | 890–915 (ПС)<br>935–960 (БС) | 200 | 300 (БС) | 124 | 200KF7W GMSK |
| DCS-1800 | 1710–1785 (ПС)<br>1805–1880 (БС) | 200 | <1 Вт (ПС) | 374 | 200KF7W GMSK |
| IS-95 | 825–850 (ПС)<br>870–894 (БС) | 1250 | 50 (БС) 6 (ПС) | 55 на одной несущей | 1M25B1W QPSK (БС), OQPSK(nC) |

***Примечание:*** *ПС — подвижная станция, БС — базовая станция*

Отслеживая перемещения звонившего от одной вышки к другой, можно составить маршрут его следования с погрешностью до 300–500 метров. Последний пример успешного использования системы биллинга — задержание предполагаемых убийц первого заместителя председателя Центробанка России Андрея Козлова. Сотрудники милиции, уладив процессуальные формальности, связались со всеми сотовыми операторами и запросили у них данные о том, в зоне каких базовых станций находится место преступления. Затем были получены все номера телефонов, абоненты которых выходили на связь с этого места. Работа по установлению всех звонивших заняла бы несколько месяцев, однако оперативникам повезло — один из киллеров, опасаясь, что его убьют заказчики преступления, явился с повинной. Правда, к этому времени сыщики уже имели информацию, что один из абонентов, выходивший на связь с места убийства, ранее засветился у офиса Центрального банка России. То есть преступник со своим чистосердечным признанием опередил милиционеров буквально на несколько дней.

Профессионалы утверждают, что достаточно одного звонка, чтобы квалифицированные «технари» получили необходимую информацию. Даже если объект сделает всего один звонок, а потом выключит телефон и избавится от него, будет установлено место последнего соединения и номер, по которому оно осуществлялось.

В настоящее время информацию, снимаемую с мобильных телефонов, активнее других используют частные детективы, частные охранные структуры и службы безопасности. Безусловно, тут целый букет нарушений статей Уголовного кодекса, а посему информация хорошо оплачивается. Сегодня приобрести распечатку контактов интересующего абонента можно двумя способами. Первый — напрямую купить ее у «своих» людей в сотовой компании. Впрочем, сделать это достаточно проблематично — службы безопасности операторов сотовой связи постоянно борются с такими утечками. Тут уместно будет вспомнить одну забавную историю. Как известно, данные биллинга — это основной инструмент при сборе информации о тех же супружеских изменах. Так вот, добыв неопровержимые доказательства неверности мужа, одна женщина в слезах швырнула супругу в лицо полученную у детектива распечатку телефонных разговоров и хлопнула дверью. Изобличенный ловелас взял детализацию, отправился в свою сотовую компанию и устроил страшный скандал. В результате служба безопасности компании очень быстро вычислила «крота», и канал получения распечаток для целого детективного агентства был закрыт. С тех пор детективы никому не дают на руки плоды своего труда... В среднем сегодня получение детализации одного телефонного номера (на профессиональном сленге — «деталь») обходится в 500 долларов. Ее анализ — установление контактов абонента, его перемещения и прочее — минимум в 1,5 тысячи долларов. Однако, для того чтобы заинтересовать человека в сотовой компании, нужно постоянно запрашивать большой объем номеров, а это бывает не всегда.

Есть и другой путь — попросить знакомых оперативников включить в список подаваемых на пробивку номеров мобильных телефонов и интересующие номера. Правда, по некоторым причинам организационного и технического характера этот процесс может растянуться до одной недели, а значит, заказчик потеряет время и, возможно, упустит прибыль. Впрочем, все работающие в этой области отмечают, что получать информацию с каждым днем становится труднее. Последняя перетряска в том же МВД лишила доступа к данной услуге очень многих. Сотовые компании все больше внимания уделяют защите информации о своих клиентах. Кроме того, по словам представителя компании, защита клиентов от несанкционированного прослушивания во время разговоров обеспечивается в рамках самого стандарта сотовой связи GSM, который осуществляет потоковое кодирование голоса и данных при их передаче.

Увы, как это часто бывает, современные технические средства используют не только спецслужбы, милиция и охрана, но и те, с кем они борются. Правоохранительные органы располагают данными

о том, что система биллинга используется злоумышленниками при подготовке серьезных преступлений — убийств, похищений или крупных ограблений. Кстати, как правило, занимаются этим бывшие сотрудники спецслужб, имеющие навыки оперативно-розыскной деятельности. При расследовании некоторых громких заказных убийств сотрудники правоохранительных органов находили у исполнителей и заказчиков преступлений распечатки детализаций сотовых телефонов жертв и записи их разговоров.

На вопрос корреспондента «Итогов», можно ли как-то защититься от биллингового слежения и «прослушки», сотрудник крупной сотовой компании на полном серьезе ответил: «Можно. Никогда не пользоваться мобильным телефоном». Интересно, сколько человек сегодня смогут последовать этому совету? Точно не многие. Хотя есть охраняемые, которые не пользуются телефоном вообще, решая все вопросы через удаленных помощников. Но таких единицы. Большинство либо часто меняет телефоны, известен случай, когда один клиент в горячей ситуации менял телефоны каждые сорок минут, либо используют специальные телефоны со сменным «эмеем», сигнализацией о попытке «прослушки», и автоматическим отключением после сработки сигнализации. Понятно, что такие телефоны стоят на порядок дороже обычных.

Каждый выбирает свой путь защиты. Но, как уже было сказано, мобильный телефон сегодня — это главное оружие противника по выуживанию информации о месте нахождения объекта (например, охраняемого лица и его охраны) и его делах.

**Сегодня при помощи телефона возможно:**

Визуальное фотографирование окружающих лиц и предметов.

Видеосъемка и акустический контроль в радиусе до 10 метров от мобильного телефона с последующей регистрацией всех говорящих.

Прослушивание всех входящих и исходящих телефонных разговоров, СМС и электронной почты и скрупулезная архивация всей информации.

Четко определять местоположение объекта (мобильника) с точностью до нескольких метров.

Дистанционное включение микрофона с расстояния в десятки тысяч километров.

Дистанционное прослушивание разговоров через микрофон телефона, даже если основная батарея извлечена.

Определить, что включился ваш микрофон, практически очень сложно, и злоумышленник спокойно может слышать и записывать не только ваши разговоры по телефону, но и разговоры в помещении, где

находится мобильный телефон. Таким образом, к вашему мобильному телефону, очень престижному и элегантному, совершенно спокойно могут подключиться не только спецслужбы (естественно, в соответствии с законом), но и большое количество конкурентов с целью получения сведений о вас, в том числе и компромата. Недаром в газете «Московский комсомолец» как-то написали, что компромат в России стал очень дешев, несколько тысяч долларов. «Подглядывать» и «прослушивать» стало очень дешево. Не в этом ли причина?

Другой возможный вариант применения «мобильника» — подбросить его в нужное помещение или подарить интересующему лицу, скажем, на день рождения.

В первом случае принцип работы устройства следующий. Преступник оставляет мобильный телефон в комнате или автомобиле. Как только аппарат фиксирует движение (а он это умеет), владелец получает соответствующее сообщение. Микрофон устройства можно активизировать извне, просто позвонив. При этом телефон никак не отреагирует на входящий звонок. Разговор в помещении можно, таким образом, не только услышать в «прямом эфире», но и записать.

Помимо записи беседы, телефон может автоматически определять движение рядом с собой и фотографировать объект. Снимки при этом могут храниться на карточке памяти, и их можно отсылать при помощи GPRS. Примечательно, что режим работы «невидимый». При активации этого режима телефон будет выглядеть отключенным, однако те, кому нужно, все равно смогут на него позвонить.

Во втором случае объект носит подарок с собой. Прослушивание осуществляется постоянно или периодически, путем дистанционного включения. Второй вариант естественно предпочтительнее. Главным образом из-за времени прослушивания. В первом случае оно будет ограничено временем работы аккумуляторной батареи. Во втором же объект сам будет следить за зарядкой телефона. Правда, подарить телефон, если у объекта квалифицированная охрана, сложно. Но возможно. Особенно, если подарить очень дорогую модель. Тут объект может «сломаться». Жадность и понты могут сделать свое «черное дело».

**Программно-аппаратные комплексы для перехвата разговоров, ведущихся по сотовым телефонам.**

Для перехвата разговоров, ведущихся с использованием телефонов сотовой связи, используются также и специальные комплексы перехвата систем сотовой связи. Например, **система GSS-ProA** способна перехватывать разговоры по GSM-телефонам по всему миру — в сетях 900/1800/1900 МГц. Она перехватывает одновременно сиг-

нал базовой станции и мобильной станции независимо друг от друга. Автоматически или вручную системой будет произведена запись разговора между двумя телефонами объектов одновременно, а разговор будет сохранен в виде стандартного WAV-файла.

Современные комплексы перехвата систем сотовой связи могут обеспечить (в зависимости от конфигурации) слежение за управляющими (вызывными) каналами до 21 соты одновременно, позволяют контролировать и регистрировать телефонные разговоры 10 и более выбранных абонентов.

**Комплексы выпускаются в трех видах:** «карманном» (в виде сотового телефона), мобильном (в виде компактного блока, ноутбука и антенны) и стационарном (в виде настольного блока).

Кроме регистрации контролируемых переговоров комплексы могут комплектоваться (в зависимости от стандарта) некоторыми дополнительными функциями: контроля переговоров по заданному номеру, «сканирования» телефонов и перехвата входящей связи контролируемого абонента.

Для «карманного» варианта возможен контроль разговоров одного абонента в зоне действия соты. Для мобильного — одновременный контроль и запись переговоров одного (нескольких) абонентов в зоне действия нескольких сот и возможно ведение базы данных по наблюдаемым сотам. Для стационарного варианта возможны одновременный контроль и запись переговоров более десяти абонентов во всей сотовой сети и ведение расширенной базы данных.

Функция «сканирования» телефонов используется для скрытого определения телефонного номера и служебных параметров какого-либо телефона.

В случае использования функции перехвата входящей связи контролируемого телефона возможен перехват всех входящих звонков заданного абонента.

**Основные функции стандартного комплекса:**

- декодирование служебного канала для выявления номера мобильного телефона, по которому ведется разговор;
- прослушивание непосредственно телефонного разговора;
- возможность одновременного контроля по частоте базовой станции и частоте мобильной трубки, то есть обеспечение стабильной слышимости обоих собеседников;
- возможность одновременного контроля как по входящим, так и по исходящим звонкам;
- слежение за изменением частоты и сопровождение разговора при переезде абонента из соты в соту;

– контроль нескольких сот из одной точки;
– запись телефонных переговоров с помощью звукозаписывающей аппаратуры в автоматическом режиме;
– фиксация на жестком диске номеров мобильных телефонов, производивших переговоры во всей системе сотовой связи с указанием даты и времени.

**На мониторе в процессе работы комплекса отображаются:**
– номера всех телефонов, вызываемых по всем сотам системы;
– номера телефонов, вышедших на связь в соте, на которую настроен канал контроля, а также служебная информация.

**Программно-аппаратные комплексы используются также для перехвата пейджинговых сообщений.**

**В состав типового комплекса входят:**
– доработанный сканирующий приемник;
– компьютер с устройством преобразования входного сигнала;
– программное обеспечение.

**Комплекс позволяет решать следующие основные задачи:**
– осуществлять прием и декодирование текстовых и цифровых сообщений, передаваемых в системах радиопейджинговой связи, сохранять все принятые сообщения на жестком диске в архивном файле;
– производить фильтрацию общего потока сообщений, выделение данных, адресованных одному или ряду конкретных абонентов по априорно известным или экспериментально определенным кеп-кодам, оперативное изменение параметров списка наблюдаемых абонентов;
– осуществлять русификацию всего входного потока сообщений или адресованных только конкретным абонентам, включаемым в список наблюдаемых;
– производить обработку файлов выходных данных в любом текстовом редакторе с реализацией стандартной функции поиска по введенной строке символов и печатью необходимых данных на принтере.

**В процессе работы программы на экране монитора отображаются:**
– принимаемые по одному из активных каналов сообщения (номер отображаемого канала вводится оператором с клавиатуры без прерывания работы программы);

– текущее время суток и дата;
– время и дата приема каждого отобранного сообщения, его порядковый номер, а также идентификатор соответствующего признака отбора.

**В) Беспроводные телефоны (радиотелефоны)**

Системы беспроводных телефонов (БПТ) на первоначальном этапе своего развития предназначались в основном для замены шнура телефонной трубки беспроводной линией радиосвязи с целью обеспечения большей мобильности абонента. Дальнейшее развитие этого вида связи, особенно переход на цифровые методы обработки информации, значительно расширило область применения БПТ.

В системах БПТ аналогового типа, наиболее часто используемых в жилых помещениях и небольших учреждениях, применяются БПТ индивидуального пользования, состоящие из базовой станции, подключенной к городской телефонной сети, и переносного радиотелефонного аппарата. При использовании БПТ в крупных компаниях в качестве внутриучрежденческого средства связи организуются разветвленные сети маломощных радиотелефонов, принцип работы которых аналогичен сотовым сетям. В этих системах используются в основном цифровые методы обработки сигнала, обеспечивающие более стойкое шифрование передаваемых сообщений.

Как аналоговые, так и цифровые беспроводные телефоны работают в дуплексном режиме по нескольким каналам, причем выбор канала осуществляется автоматически из числа незанятых. Дальность действия сертифицированных радиопередатчиков (мощность излучения не превышает 10 мВт) БПТ в зависимости от типа аппаратуры и условий эксплуатации составляет 25 – 200 м.

Перечень частотных полос, выделенных для БПТ на условии ограничения максимальной выходной мощности 10 мВт и на вторичной основе, т. е. без каких-либо гарантий чистоты эфира, представлен в табл. 6.

*Таблица 6*

**Перечень частотных полос, выделенных для беспроводных телефонов мощностью до 10 мВт**

| Стандарт | Частотный диапазон, МГц |
|---|---|
| CT-0R | 30 – 31/39 – 40 |
| CT-1R | 814 – 815/904 – 905 |
| CT-2R | 864 – 868,2 |
| DECT | 1880 – 1900 |

**Фактически аналоговые БПТ на территории России работают в следующих основных диапазонах частот:**

26,3125 – 26,4875 МГц/41,3125 – 41,4875 МГц;
30,075 – 30,300 МГц/39,775 – 40,000 МГц;
31,0125 – 31,3375 МГц/39,9125 – 40,2375 МГц;
31,025 – 31,250 МГц/39,925 – 40,150 МГц;
31,0375 – 31,2375 МГц/39,9375 – 40,1375 МГц;
31,075 – 30,300 МГц/39,775 – 39,975 МГц;
30,175 – 30,275 МГц/39,875 – 39,975 МГц;
30,175 – 30,300 МГц/39,875 – 40,000 МГц;
307,5 – 308,0 МГц/343,5 – 344,0 МГц;
46,610 – 46,930 МГц/49,670 – 49,990 МГц;
254 МГц/380 МГц; 263 – 267 МГц/393 – 397 МГц;
264 МГц/390 МГц; 268 МГц/394 МГц;
307,5 – 308,0 МГц/343,5 – 344,0 МГц;
380 – 400 МГц/250 – 270 МГц;
814 – 815 МГц/904 – 905 МГц;
885,0125 – 886,9875 МГц/930,0125 – 931,9875 МГц;
902 – 928 МГц/902 – 928 МГц;
959,0125 – 959,9875 МГц/914, 0125 – 914,9875 МГц.

Цифровые БПТ используют следующие основные диапазоны частот:

804 – 868 МГц; 866 – 962 МГц; 1880 – 1990 МГц.

Для перехвата телефонных разговоров, ведущихся с использованием аналоговых БПТ, могут использоваться обычные сканирующие приемники.

При помощи сканеров можно прослушивать и переговоры охраны по радиостанциям. Радиостанции, оснащенные скремблерами, в наше время в охранных структурах встречаются редко. Почему? Да, как обычно, денег жалко.

**Г) Интернет**


Сегодня этот канал связи просто кладезь для преступников. Благодаря Интернету можно путем взлома вашего компьютера получить доступ к любой хранящейся в нем информации, а можно, наоборот, уничтожить ее, запустив вам вирус. Причем речь необязательно идет об одном компьютере, чаще — о целых компьютерных сетях. «Хакерские

дела» гремят по всему миру. 25 марта 2010 года во Франции задержан 25-летний житель французского региона Овернь, который взломал личные страницы президента США Барака Обамы в социальной сети Twitter. Молодому человеку удалось подобрать пароли к аккаунту Обамы. О результатах своей деятельности молодой человек написал в интернет-дневнике. Как отмечают в полиции Франции, хакер сказал ее работникам, что взломал интернет-страницы американского президента «из-за стремления к риску». Теперь молодому человеку грозит до двух лет тюрьмы. Подобные инциденты происходят довольно часто — молодые специалисты, движимые жаждой славы, идут на противозаконные действия, а затем оповещают об этом общественность.

Но этот случай можно отнести к разряду безобидных. На самом деле последствия деятельности хакеров могут быть весьма впечатляющими.

Кто же такие хакеры и что они могут?

Термин «хакер» раньше использовался для обозначения высококвалифицированных программистов. Теперь так называют тех, кто использует уязвимости в программном обеспечении для внедрения в компьютерную систему. Это электронный эквивалент взлома помещения. Хакеры постоянно взламывают как отдельные компьютеры, так и крупные сети. Получив доступ к системе, они крадут конфиденциальные данные или устанавливают вредоносные программы. Они также используют взломанные компьютеры для рассылки спама.

Современные приложения чрезвычайно сложны; они компилируются из тысяч строк кода. Но создаются они людьми, а людям свойственно ошибаться. Поэтому нет ничего удивительного в том, что в программы закрадываются ошибки, что делает их уязвимыми для атаки. Хакерам эти лазейки позволяют проникнуть в систему, а вирусописатели используют ошибки в коде приложений, чтобы обеспечить автоматический запуск на компьютере вредоносных программ.

Яркий пример — известный ныне хакер Кевин Митник, который взломал телефонную станцию Computer System for Mainframe Operations (COSMOS), принадлежащую компании Pacific Bell в Лос-Анджелесе. Вторгшись в систему, он переключал телефонные линии и перехватывал все звонки, идущие через эту станцию.

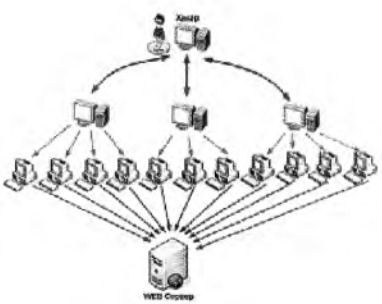
Но на этом не остановился. Хакер сумел войти в базу данных компании и украсть информацию о нескольких абонентах. Он с легкостью получил доступ к телефонным счетам, паролям, комбинациям шлюзов и даже к системному руководству. Митник даже использовал переключение телефонных линий для своих личных нужд.

1 октября 2007 года хакеры нашли способ заставить iPhone с обновленной прошивкой работать в сотовых сетях любых операторов.

Для взлома мобильника требуется SIM-карта TurboSIM и одно из платных приложений для активации iPhone либо оригинальная SIM-карта AT&T и программа iNdependence. Использовав один из этих методов, владелец iPhone получает полнофункциональный обновленный мобильник, не привязанный к какому-либо оператору, несмотря на все старания инженеров Apple.

Напомним, коммуникатор iPhone появился в продаже в конце июня 2007 года. Одним из недостатков мобильника СМИ называли необходимость заключать при покупке двухгодичный контракт с AT&T и, соответственно, пользоваться определенным оператором только одной страны. Для обнаружения способа взлома этой блокировки хакерам потребовалось всего два месяца.

24 декабря 2008 года в Рунете произошла череда сбоев с доступом к известным ресурсам. Технические сбои разной степени тяжести испытывали сайты оппозиции «Грани.ру», «Каспаров.ру» и «Нацбол.ру» и социальная сеть «Одноклассники».



18 июня 2009 года неизвестные злоумышленники осуществили массированную хакерскую атаку, в ходе которой внедрили вредоносный программный код более чем в 40 тысяч веб-сайтов.

Посетители взломанных сайтов через цепочку серверов автоматически перенаправлялись на страницу, содержащую эксплойты для уязвимостей в программном обеспечении компаний Adobe, Apple и Microsoft. Если компьютер жертвы оказывается уязвимым, на него загружались троянские программы и прочие вредоносные модули.

Атака получила название Nine-Ball — по имени конечного сайта, на который переадресовываются пользователи. До сих пор неясно, каким именно образом злоумышленникам удалось взломать несколько десятков тысяч сетевых ресурсов. Эксперты Websense считают, что киберпреступники тем или иным незаконным способом получили логины и пароли для доступа к серверам, обслуживающим сайты-мишени, и затем внедрили в них свой программный код.

В феврале 2010 года компания ScanSafe сообщила, что хакерские атаки 2009 года, направленные на программное обеспечение, чаще всего затрагивали уязвимости в пакете Acrobat и приложении Acrobat Reader компании Adobe Systems. По оценкам компании, в четвертом квартале зараженные документы в формате Adobe PDF применялись в 80 процентах хакерских атак.


На протяжении всего 2009 года аналитики американской фирмы по компьютерной безопасности отмечали рост доли PDF-файлов в общем числе хакерских атак. В первом квартале она составила 56 процентов от всех эксплойтов, обнаруженных ScanSafe. Во втором и третьем кварталах доля превысила 60 и 70 процентов соответственно.

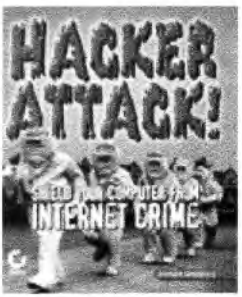
По мнению специалистов, хакерские нападения на пользовательские компьютерные системы посредством уязвимостей в Acrobat обусловлены в первую очередь огромной популярностью PDF-файлов как универсального формата документов.

Результатом повышенного внимания хакеров к программам Adobe стал рост числа обнаруженных уязвимостей. Так, по данным публичной базы данных уязвимостей и незащищенностей Common Vulnerabilities and Exposures (CVE), в 2006 году количество обнаруженных Acrobat-дефектов составляло 35, через два года их уже было выявлено 58, а в 2009-м — 107.

18 февраля 2010 года специалисты по кибербезопасности обнаружили новую глобальную хакерскую атаку, в ходе которой были взломаны системы почти 2500 компаний и похищены огромные объемы данных. Атаки осуществляли хорошо организованные хакерские группы из Европы и Китая.

Как отмечают специалисты NetWitness (компания занимается анализом безопасности компьютерных сетей), ущерб от последних кибератак все еще оценивается, а пострадавшие организации вычисляются. По имеющимся сейчас сведениям, хакеры похитили данные 2411 компаний разного профиля. Среди украденной информации данные о транзакциях по кредитным картам, интеллектуальная собственность и многое другое.

Также неизвестным киберпреступникам удалось проникнуть в сети десяти государственных организаций США. В одной из компаний хакеры получили доступ к корпоративному серверу, который занимался обработкой платежей по кредитным картам. В еще одном случае характер атаки позволил установить очевидное участие во взломе одного из сотрудников самой компании.




Так что государственный пост от хакеров тоже не защищает.

Вопросы о безопасности правительственных веб-сайтов в той же Америке становятся все более острыми. Все больше сайтов, адреса которых заканчиваются на .gov, подвергаются атакам хакеров, размещающих на них ссылки на сайты с порно и вредоносным ПО.

В список жертв злоумышленников вошел сайт Marin County Transportation Authority. Представители организации обнаружили, что атаки на сайт удвоились. В начале октября многочисленные атаки калифорнийских правительственных веб-сайтов сильно нарушили их работу. Работа сайтов была парализована. Эти сайты пришлось закрыть до тех пор, пока администраторы не удалили ссылки, размещенные злоумышленниками. Спустя неделю после того, как сайты были реанимированы, ссылки появились вновь. Другим сайтом, «зараженным» ссылками на порно и вредоносное ПО, стал USAid, сайт федерального агентства, предоставляющего помощь странам, пострадавшим от бедствий.

Не лучшим образом обстоят дела и в России. В 2009 году сотрудники Федеральной службы безопасности отразили 1,2 миллиона хакерских атак, причем 280 тысяч из них пришлось на сайт президента, сообщил директор ФСБ Александр Бортников на традиционной встрече с главными редакторами ведущих российских СМИ, приуроченной ко Дню сотрудников органов госбезопасности.

По словам главы ФСБ, в целях обеспечения информационной безопасности было возбуждено свыше 230 уголовных дел и осуждено более 20 человек. Он, в частности, назвал участников международных хакерских групп россиян Андриянова, Полудкина, Соколова и Ширяева, а также граждан Болгарии Божилова и Илиева. Они подделывали кредитные карты и пытались снимать с их помощью деньги со счетов настоящих владельцев.

Надо отметить, что спецслужбы различных государств также не чужды «хакерства». Более того, интернет-пространство рассматривается ими как реальное поле боя. В середине ноября 2009 года Конгрессу Соединенных Штатов был представлен отчет специальной комиссии по американо-китайским экономическим отношениям, в котором отмечается, что Китай всерьез готовится к цифровой войне с США.

По сведениям генерала Джеймса Картрайта, возглавляющего отдел стратегического командования армии США, в случае гипотети-

ческих военных действий между двумя странами Китай способен провести эффективные кибератаки на региональные базы США в Японии и Южной Корее. Более того, Китай обладает всеми средствами для атак на сетевую инфраструктуру на территории США, что может подорвать экономическую, телекоммуникационную и энергетическую стабильность в стране.

Картрайт подчеркнул, что уже сейчас спецслужбы Китая изучают телекоммуникационную инфраструктуру США на предмет обнаружения слабых мест в цифровой защите. Генерал убежден, что хорошо спланированную кибератаку на сети противника можно смело назвать оружием массового поражения. В свете этой информации, Картрайт настоятельно порекомендовал Конгрессу обратить на эту проблему особое внимание.

Тем более что уже известно несколько случаев успешных хакерских атак на правительственные сети, осуществленные, предположительно, с китайской стороны. В частности, в сентябре 2009 года был неожиданно отключен сегмент сети Пентагона, обслуживающий министра обороны США Роберта Гейтса.

**Как обнаружить хакерскую атаку**

Есть множество способов воспользоваться большинством уязвимостей. Для хакерской атаки можно использовать один эксплойт, несколько эксплойтов одновременно, неверные настройки программных компонентов или даже программу-бэкдор, установленную в операционную систему в процессе предыдущей атаки.

Из-за этого детектирование хакерской атаки становится не самой простой задачей, особенно для неопытного пользователя. В этом разделе мы постараемся сформулировать советы, способные помочь читателю определить, подвергается ли его компьютер хакерской атаке или же защита компьютера уже была взломана ранее. Помните, что, как и в случае вирусов, никто не дает 100% гарантии, что вы сможете зафиксировать хакерскую атаку подобными способами. Впрочем, если ваша система уже взломана, то вы наверняка отметите некоторые из нижеприведенных признаков.

**Windows-компьютеры**

*Подозрительно высокий исходящий трафик.* Если вы пользуетесь дайлапом или ADSL-подключением и заметили необычно большое количество исходящего сетевого трафика (в частности, проявляющегося, когда ваш компьютер работает и подключен к Интернету, но вы им не пользуетесь), то ваш компьютер, возможно, был

взломан. Такой компьютер может использоваться для скрытой рассылки спама или для размножения сетевых червей.

*Повышенная активность жестких дисков или подозрительные файлы в корневых директориях.* Многие хакеры после взлома компьютера производят сканирование хранящейся на нем информации в поисках интересных документов или файлов, содержащих логины и пароли к банковским расчетным центрам или системам электронных платежей вроде PayPal. Некоторые сетевые черви схожим образом ищут на диске файлы с адресами e-mail, которые впоследствии используются для рассылки зараженных писем. Если вы заметили значительную активность жестких дисков, даже когда компьютер стоит без работы, а в общедоступных папках стали появляться файлы с подозрительными названиями, это также может быть признаком взлома компьютера или заражения его операционной системы вредоносной программой.

*Большое количество пакетов с одного и того же адреса, останавливаемые персональным межсетевым экраном.* После определения цели (например, диапазона IP-адресов какой-либо компании или домашней сети) хакеры обычно запускают автоматические сканеры, пытающиеся использовать набор различных эксплойтов для проникновения в систему. Если вы запустите персональный межсетевой экран (фундаментальный инструмент в защите от хакерских атак) и заметите нехарактерно высокое количество остановленных пакетов с одного и того же адреса, то это — признак того, что ваш компьютер атакуют. Впрочем, если ваш межсетевой экран сообщает об остановке подобных пакетов, то компьютер, скорее всего, в безопасности. Однако многое зависит от того, какие запущенные сервисы открыты для доступа из Интернета. Так, например, персональный межсетевой экран может и не справиться с атакой, направленной на работающий на вашем компьютере FTP-сервис. В данном случае решением проблемы является временная полная блокировка опасных пакетов до тех пор, пока не прекратятся попытки соединения. Большинство персональных межсетевых экранов обладают подобной функцией.

Постоянная антивирусная защита вашего компьютера сообщает о присутствии на компьютере троянских программ или бэкдоров, хотя в остальном все работает нормально. Хоть хакерские атаки могут быть сложными и необычными, большинство взломщиков полагается на хорошо известные троянские утилиты, позволяющие получить полный контроль над зараженным компьютером. Если ваш антивирус сообщает о поимке подобных вредоносных программ, то это может быть признаком того, что ваш компьютер открыт для несанкционированного удаленного доступа.

**UNIX-компьютеры**

*Файлы с подозрительными названиями в папке «/tmp».* Множество эксплойтов в мире UNIX полагается на создание временных файлов в стандартной папке «/tmp», которые не всегда удаляются после взлома системы. Это же справедливо для некоторых червей, заражающих UNIX-системы; они рекомпилируют себя в папке «/tmp» и затем используют ее в качестве «домашней».

*Модифицированные исполняемые файлы системных сервисов вроде «login», «telnet», «ftp», «finger» или даже более сложных типа «sshd», «ftpd» и других.* После проникновения в систему хакер обычно предпринимает попытку укорениться в ней, поместив бэкдор в один из сервисов, доступных из Интернета, или изменив стандартные системные утилиты, используемые для подключения к другим компьютерам. Подобные модифицированные исполняемые файлы обычно входят в состав rootkit и скрыты от простого прямого изучения. В любом случае полезно хранить базу с контрольными суммами всех системных утилит и периодически, отключившись от Интернета, в режиме одного пользователя, проверять, не изменились ли они.

*Модифицированные «/etc/passwd», «/etc/shadow» или иные системные файлы в папке «/etc».* Иногда результатом хакерской атаки становится появление еще одного пользователя в файле «/etc/passwd», который может удаленно зайти в систему позже. Следите за всеми изменениями файла с паролями, особенно за появлением пользователей с подозрительными логинами.

*Появление подозрительных сервисов в «/etc/services».* Установка бэкдора в UNIX-системе зачастую осуществляется путем добавления двух текстовых строк в файлы «/etc/services» и «/etc/inetd.conf». Следует постоянно следить за этими файлами, чтобы не пропустить момент появления там новых строк, устанавливающих бэкдор на ранее неиспользуемый или подозрительный порт.

**Как защитить компьютер от хакерских атак?**

Итак, хакеры — это электронные взломщики, которые проникают в вашу компьютерную систему, используя особые лазейки — уязвимости в программном обеспечении. Защищаться от них специалисты рекомендуют с помощью особого приложения — сетевого экрана. Сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа.

Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определенные в конфигурации.

Экран обычно входит в состав антивирусных программ. Он распознает попытки взлома и делает ваш компьютер невидимым для хакеров.

Но на самом деле все не так радужно, поскольку вредоносные программы производятся тысячами, а антивирусные разрабатываются по факту. То есть налицо очередное битье по хвостам. Сначала вас атаковали, а затем разрабатывается антивирусная программа для борьбы с новым вирусом. Вашего клиента сильно обрадует, если его бизнес рухнет, а на его примере потом разработают меры противодействия? Точно. Нет.

Поэтому вопрос компьютеризации вашей компании и ее компьютерной безопасности — это вопрос вопросов.

*При написании данной главы были использованы материалы статей А.А. Хорева*

# Глава 3. Технические средства несанкционированного съема информации

В предыдущей главе мы рассмотрели основные каналы утечки информации, где упоминали различные технические средства съема информации. Давайте познакомимся с ними поближе.

## 3.1. Устройства несанкционированного съема аудиоинформации (УНСАИ) – жучки

### Сверхминиатюрный жучок + телефонный жучок

Универсальное устройство 2 в 1 «Сверхминиатюрный жучок + телефонный жучок» обладает функциями двух устройств и предназначено для прослушивания разговоров в помещении и прослушивания телефонных разговоров. Оно является одним из самых миниатюрных в мире записывающих устройств, его размеры — 7×20×34 мм. Данное устройство мультифункционально, очень просто в обращении и обладает профессиональными характеристиками. Максимальное время записываемой информации (объем памяти) составляет 150,3 часа записи. Устройство имеет настолько сверхчувствительный микрофон и настолько высокое качество записи, что позволяет при включенном выносном микрофоне качественно записывать разговоры даже из закрытого металлического сейфа.

**Характеристики устройства:**

Размеры — 7×20×34 мм, вес — 10 граммов.

Количество записываемой информации — до 150 часов. После заполнения памяти вы можете перенести записи на компьютер, стереть их и записывать снова.

Принцип записи — встроенная flash-память. Источник питания — литиево-ионный аккумулятор.

Время непрерывной работы (записи или прослушивания записанной информации) в режиме записи/в дежурном режиме — 30 ч / 1,5 месяца.

**При записи разговоров в помещении:**

Вы оставляете устройство в помещении, в котором нужно скрыто записать разговоры, активируете запись нажатием кнопки. Индикатор покажет, что запись началась.

Устройство имеет ультраминиатюрные размеры, так что обнаружить его практически невозможно. При помощи оборудования для поиска прослушивающих устройств обнаружить его также невозможно, так как он работает по другому принципу. После того, как нужная информация записана, вы забираете устройство.

**Далее вы сможете:**

Прослушать записанную информацию через наушник, входящий в комплект.

Перенести записанную информацию в компьютер при помощи USB-адаптера и программного обеспечения, входящих в комплект.

Очистить память и записывать заново.

Устройство имеет сверхчувствительный встроенный микрофон, позволяющий записывать разговоры в радиусе 10 метров.

Есть возможность регулировать качество записи и чувствительность микрофона.

Во время записи работает функция «Сжатие пауз». Устройство воспринимает абсолютную тишину как паузу и сжимает ее, чтобы паузы не занимали места в памяти.

**При записи с телефонной линии:**

При помощи функции «Активация голосом» устройство записывает только разговоры, без пауз. Запись начинается при поднятии трубки и приостанавливается по окончании разговора. Далее запись активируется при начале следующего разговора.

Каждый разговор будет записан как отдельный файл.

При записи с телефонной линии работает функция АОН (автоматическое определение номера), позволяющая определить номер звонящего абонента.

При записи телефонных разговоров устройство подзаряжается от телефонной линии и может записывать телефонные разговоры до полного заполнения памяти.

Подключить устройство к телефонной линии можно в любом месте как в телефонную розетку, так и в телефонный щиток в подъезде.

### Жучок + телефонный жучок с беспроводным радиомикрофоном

Устройство «Жучок + телефонный жучок с беспроводным радиомикрофоном» сочетает в себе устройство для скрытой записи и прослушивания разговоров в помещении (устройство снабжено уникальным беспроводным радиомикрофоном, который может быть установлен на расстоянии до 20 метров от самого устройства!) и устройство для скрытой записи телефонных переговоров.

Уникальный радиомикрофон, входящий в комплект поставки, позволит установить, например, само устройство в одном помещении, а радиомикрофон в соседнем помещении.

Время максимальной записи (объем памяти) — до 282 часов записи.

**Характеристики устройства:**

Размеры — 39×96×12 мм.

Вес — 37 граммов.

Количество записываемой информации — до 282 часов.

После заполнения памяти вы можете перенести записи на компьютер, стереть их и записывать снова.

Принцип записи — встроенная flash-память 1024 Mb. Источник питания — батарея AAA.

Время непрерывной работы (записи или прослушивания записанной информации) в режиме записи/в дежурном режиме — 10 часов. Время работы увеличивается при включенной функции «Активация голосом».

**При записи разговоров в помещении:**

Вы оставляете устройство в помещении, в котором нужно скрыто записать разговоры, активируете запись нажатием кнопки. Индикатор покажет, что запись началась.

Вы, конечно, можете оставить в интересующем помещении само устройство, но!

Беспроводной радиомикрофон позволяет включить само устройство в одном помещении, а беспроводной радиомикрофон в соседнем помещении (на расстоянии до 20 метров, например в соседней комнате или в соседнем кабинете сотрудника).

При таком способе записи не придется заходить в помещение, в котором оставлен беспроводной радиомикрофон для замены батареи. После того, как нужная информация записана, вы забираете устройство.

**Далее вы сможете:**

Прослушать записанную информацию через наушник, входящий в комплект.

Перенести записанную информацию в компьютер при помощи USB-адаптера и программного обеспечения, входящих в комплект.

Очистить память и записывать заново.

Функция «Активация голосом» позволяет записывать только разговоры, без пауз (устройство воспринимает тишину как паузу и не записывает ее, это позволяет экономить место в памяти и энергию).

Функция «Автоматическое отключение» позволит экономить питание и отключать запись по расписанию.

Интеллектуальная функция шумоподавления позволяет качественно записывать разговоры, даже если на фоне работает телевизор, радиоприемник или есть какие-то другие шумы. Эта функция полезна как при записи разговоров в помещении, на улице, так и в автомобиле.

Встроенный чувствительный микрофон имеет 4 градации чувствительности + есть возможность выбора качества ведущейся записи. USB-разъем интегрирован в само устройство, так что для подключения его к компьютеру не требуется никаких кабелей и проводов.

**При записи с телефонной линии:**

При помощи функции «Активация голосом» устройство записывает только разговоры, без пауз. Запись начинается при поднятии трубки и приостанавливается по окончании разговора. Далее запись активируется при начале следующего разговора.

Каждый разговор будет записан как отдельный файл.

Подключить устройство к телефонной линии можно в любом месте как в телефонную розетку, так и в телефонный щиток в подъезде.

**Где могут прятаться жучки?**

При ответе на этот вопрос надо учитывать, что в основном жучки делаются вручную и каждый мастер использует какие-то свои находки. Поэтому ответ на этот вопрос сложен настолько, что просто может не хватить фантазии, на что будет способен очередной «Кулибин» при изготовлении своего очередного шедевра. Хотя общие черты все же можно обрисовать.

*Во-первых*: нужно внимательно осматривать все розетки, провода и прочее, где есть электричество, потому что жучок, установленный в ваше отсутствие таким образом, имеет постоянное питание и может работать сколь угодно долго, это важно, потому что жизнь жучка, работающего от батареек, ограниченна.

*Во-вторых*: очень внимательно проверяйте подарки, которые вам дарят деловые партнеры и просто коллеги. Известен случай, когда американскому послу был вручен от «советских пионеров» герб США, сделанный из ценных пород дерева, в котором находился жучок. Дипломат повесил его у себя в кабинете, и «пионеры с Лубянки» в течение 15 лет были в курсе всех секретов американской политики.

*В-третьих*: очень внимательно относитесь к «случайно» забытым вещам (барсеткам, ручкам и так далее) или непонятно откуда появившимся у вас предметам, вполне возможно, что в новой пепельнице или тройнике в розетке запрятан жук.

*В-четвертых*: не поленитесь купить недорогой магнитофон и во время переговоров или важных совещаний включать фоновую музыку, это, конечно, не спасет от всех бед, но может забить ваш разговор посторонним шумом.

*В-пятых*: при осмотре помещения с помощью технических средств не надейтесь, что из прибора выскочит маленький человечек и укажет вам место, где сидит жучок. Все гораздо сложнее: вам нужно набраться изрядного терпения в обследовании вашего помещения и облазить всевозможные плинтуса, карнизы, заглянуть под столы и стулья. При этом важно учитывать что по мощности излучения жучки бывают разные: какой-то передает на 150 метров, а какому-то необходимо передать информацию только через стенку любопытному заму охраняемого лица, поэтому и дальность реагирования на них антижучков тоже будет разной: от 2 м в первом случае и до 10 — 20 см во втором.

Поэтому наберитесь терпения и вперед — сантиметр за сантиметром проверяйте ваше помещение, это помогает. Приведем несколько примеров.

**Ситуация:**

Жучок найден в одном из московских офисов. Сотрудники проводили плановую проверку кабинетов. Возле одной из розеток было обнаружено излучение, разобрали розетку — внутри лежало вот это. Судя по всему, прибор изготовлен профессионалами, потому что он находится в пластиковом корпусе, и, судя по пайке, это делалось на профессиональном оборудовании. В принципе, их это не удивило,


это уже второй жучок, который они находили в наших офисах — и снова в коммерческом отделе. После первого раза, когда они приглашали профессиональную проверку, они приобрели поисковое оборудование. И результат не заставил себя ждать. Самое удивительное, что время между этими жучками всего 2 месяца.

**Наши комментарии:**


Да, действительно, эта находка удивительна, мы чаще всего сталкиваемся с жучками, которые сделаны кустарно, но этот прибор сделан профессионально. Вполне возможно, данное оборудование привезено из-за рубежа, скорее всего из Тайваня, там продажа такого оборудования почти легальна и купить такой жучок там несложно. Также, судя по внешнему виду, прибор очень качественно и далеко передает информацию.

**Ситуация:**

Фирма технического профиля, жука нашел инженер на столе в комнате менеджеров, судя по всему, лежал недавно, было ощущение, что подбросили абы как, тем более что в этой комнате слушать нечего. Инженер погорячился, бросив устройство в стакан с водой, и теперь невозможно определить его технические возможности.

Приборов у сотрудников никаких не было. Жучок просто валялся на столе, не особо маскируясь, а поскольку люди технически грамотные, то сразу стало ясно, что это за устройство. Насторожившись, сотрудники вызвали знакомого с аппаратурой, облазили весь офис и нашли два странных места. В офисе все стены из гипсокартона, так вот в двух местах офиса явно присутствует какая-то аномалия на стенах, обращенных на улицу за гипсокартоном, где индикатор поля показывал наличие излучения. Локализовали источник до диаметра 30 см. Что делать? Разби-

рать стену? Что это может быть, как вы думаете? Какие дальнейшие действия? Что можно услышать через гипсокартон? Электричество отрубали полностью, гасили все, источник излучения не пропадает...

Вскоре заметили машины, стоящие напротив окон по другую сторону улицы, с сидящими в них и ничего не делающими людьми... Через некоторое время машины уезжали и источник излучения пропадал, а назавтра все повторялось опять, но уже стояла другая машина и другой человек в ней.

**Наши комментарии:**

Особенно комментировать ту нечего. Даже немного вызывает улыбку — люди заняты серьезным бизнесом и при этом наивно полагают, что они никого не интересуют и сидят в песочнице, строят из песка домики. Не бывает так. Как только появляется какая-то деятельность, а за ней и прибыль, то найдется добрый десяток недобрых людей, которым всегда будет интересно, откуда у вас деньги, как вы их заработали и как потратили. А то, что под окнами постоянно стоят машины с ничего не делающими людьми, так это уже должно наводить на определенные размышления.

**Ситуация:**

Фирма по продаже игровых автоматов. Во время довольно сложных переговоров, которые проходили в офисе, у сотрудника безопасности периодически стал пищать антижучок «Бизнес». Он, естественно, напрягся, но списал это на постоянный треск сотовых телефонов. Когда переговоры закончились, треск не прекратился, тогда он взял прибор и прошелся по комнате. В стакане с ручками нашел одну очень забавную ручку. Когда он ее разобрал — там был спрятан очень маленький жучок. Видимо, партнеры фирмы рассчитывали на то, что после того, как они уйдут, начнется активное обсуждение результатов переговоров и вся информация станет им известна. Ведь ни для кого не секрет, что после переговоров, когда вторая сторона уходит, люди начинают активно высказывать свои мнения по самим переговорам. Короче, с этой фирмой сотрудники больше дела не имели.

**Время поиска:**

Заняло где-то 10 — 15 минут, из них 5 минут, по словам сотрудника, он не мог поверить, что в ручке что-то может находиться. Ниже

представлены фотографии жучка. Этот пример показывает, что нож в спину можно ждать откуда угодно, даже из простой ручки. Будьте, пожалуйста, внимательнее, особенно после переговоров.

**Наши комментарии:**

Данная история очень показательна в том плане, что ваши конкуренты или будущие партнеры не остановятся ни перед чем ради получения заветной информации, это и подкуп, и шантаж, и даже банальное запугивание ваших работников, ну а уж подкинуть жучок к вам в офис — святое дело! При этом это может сделать и техничка, и простой сантехник.

**Ситуация:**

Сотрудник одной крупной компании менял батарейку в часах и нашел жучок. Немного удивился. Причем установлен был очень грамотно, сам жучок спрятан был в корпус часов, где расположен механизм, то есть обычно туда не влезают. При замене батареек случайно разобрал этот корпус. Как долго жучок стоял в часах — неизвестно. Часы покупал он сам и надолго никого в кабинете не оставлял. После этого случая пригласил сотрудников службы безопасности для проверки кабинета.

**Время поиска:**

Найдено случайно.

**Наши комментарии:**

Передатчик предназначен для закладки в часы. Следует обратить внимание, что передатчик устанавливается в кварцевые или электронные часы (они не тикают). Преимуществом данного передатчика является то, что нет необходимости постоянно менять батарейку, ее постоянно меняет владелец часов. Время работы передатчика неограниченно, пока он не будет обнаружен. Вместе с передатчиком обычно поставляется специальный радиоприемник с расширенным диапазоном. Диапазон работы передатчика FM 110 – 115 МГц, то есть сигнал не будет перехвачен на обычный FM-радиоприемник (обычный диапазон 88 – 108 МГц), и также полностью отсутствуют помехи FM-радиостанций.

Часы — один из самых распространенных предметов, куда ставят жучки. Установка жучка — дело нехитрое: покупаются аналогичные часы, в которые вставляется жучок. Затем часы просто меня-

ются в кабинете, пока хозяин выходит, на это уходит ровно 15 секунд. Таким же образом жучка вам могут подсунуть в калькуляторе, тройнике, мышке для компьютера и так далее.

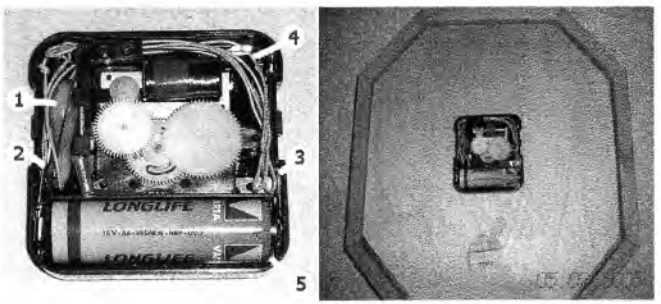


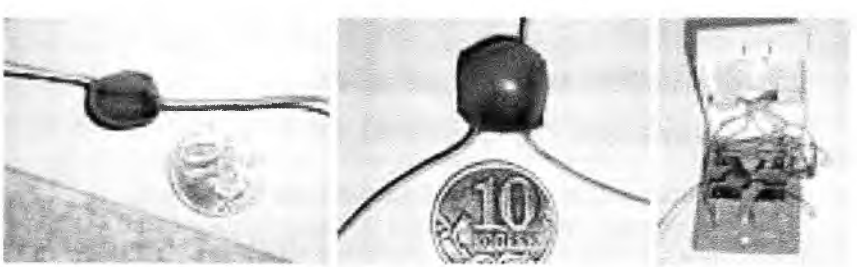

*Рис. 1.*
*1 — передатчик; 2 — крепление на минус; 3 — крепление на плюс; 4 — антенна; 5 — питание*

**Ситуация:**

Бизнесмен развелся с женой, очень долго ломал голову, откуда она знает о его похождениях. Все было непонятно, пока на Новый год ему не подарили индикатор поля. Первым делом проверил офис, но ничего не нашел. Ради интереса взял его домой, ну и вот результат: в телефонной коробке обнаружил «прослушку». Видимо, жена поставила жучок на телефон и где-то в доме стояло записывающее устройство, которое регистрировало все звонки. Когда он отнес закладку к знающим людям, они сказали, что работает он на частоте 110 FM, то есть диапазон радиоприемников 88 — 108 FM, а тут, видимо, у приемника вручную расширили диапазон, и его было невозможно поймать на простое радио. Причем, что интересно, стоял он, похоже, где-то не менее 6 месяцев и питался от телефонной сети.

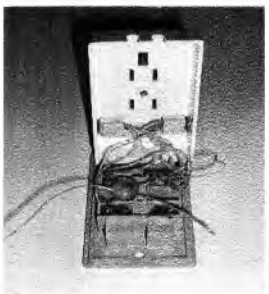
**Время поиска:**

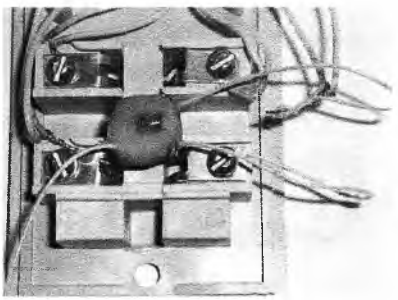
Найдено в течение 10 минут.



**Наши комментарии:**

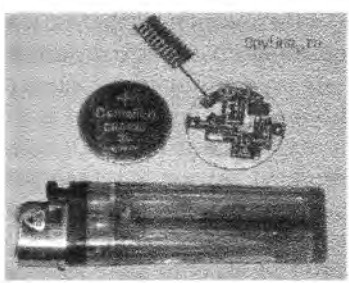
Если честно, комментировать тут особенно нечего — все налицо: две разбитые судьбы. Жучки, к сожалению, используют не только в промышленном шпионаже, но и в обычной жизни...





### Кварцованный жучок-таблетка

**Кварцованный жучок**



— одна из старейших, но в то же время одна из самых надежных и дешевых моделей. Традиционно малые размеры и вес позволяют быстро и незаметно проводить установку жучка, а небольшая стоимость позволяет в ряде случаев использовать его как расходный материал, не требующий последующего снятия.

**Функциональные особенности:**

миниатюрный размер; малый вес (от 5 граммов); частота — 400 — 430 Мгц;

микрофон с чувствительностью — до 10 метров; автономная работа — до 4 суток; дальность — до 250 — 300 м; элемент питания — круглая батарейка CR2450.

## 3.2. Миниатюрные цифровые диктофоны

### Цифровой мини-диктофон E-dic Gold-17920 мин. (300 ч)

**Профессиональные цифровые диктофоны E-dic Gold**

Самые маленькие диктофоны серии e-dic, они имеют еще меньшие габариты, чем занесенные в Книгу рекордов Гиннесса-2007 E-dic Tiny.

Металлический корпус этого диктофона очень прочен, а сам прибор для удобства можно прицепить в виде брелка. Стильный цвет E-dic Gold в сочетании с прекрасным качеством записи делают этот диктофон превосходным имиджевым подарком для делового человека.

**Функциональные особенности:**

- самый маленький размер;
- очень прост в использовании — управление одной кнопкой;
- длительное время записи;
- выносной микрофон с чувствительностью до 7 метров;
- автономная работа при непрерывной записи до 24 часов;
- функция «цифровой подписи» для защиты записанных файлов;
- активация голосом;
- возможность записи с телефона;
- широкий динамический диапазон;
- встроенный USB-интерфейс.

### Цифровой мини-диктофон E-dic Tiny-1792D мин. (300 ч)

Цифровые диктофоны E-dic Tiny — новые миниатюрные диктофоны серии e-dic. Имеют еще меньшие габариты, чем E-dic mini, и расширенные функциональные возможности. Эти микродиктофоны все так же просты, удобны, надежны в использовании и обладают высоким качеством записи.

**Функциональные особенности:**

- миниатюрный размер;
- малый вес (от 5 граммов);
- длительное время записи;
- выносной микрофон с чувствительностью до 7 метров;
- автономная работа при непрерывной записи — до 60 часов;
- возможность записи с телефона;
- функция «цифровой подписи» для защиты записанных файлов;
- активация голосом;
- широкий динамический диапазон;
- встроенный USB-интерфейс.

### Цифровой мини-диктофон E-dic LCD-17920 мин. (300 ч) E-dic LCD –


одна из последних моделей в линейке самых маленьких диктофонов в мире. Традиционно малые размеры и вес в сочетании с простым управлением, стойкостью к воздействию внешней среды, а также высокое качество записи и наличие ЖК-экрана выгодно отличают этот мини-диктофон.

**Функциональные особенности:**

- миниатюрный размер;
- малый вес (от 5 граммов);
- длительное время записи;
- выносной микрофон с чувствительностью до 7 метров;
- автономная работа при непрерывной записи — до 250 часов;
- возможность записи с телефона;
- несколько степеней сжатия речи;
- трехстрочный ЖК-экран;
- активация голосом;
- широкий динамический диапазон;
- удобное управление — джойстик;
- USB-адаптер.

**Адаптер записи телефонных переговоров**

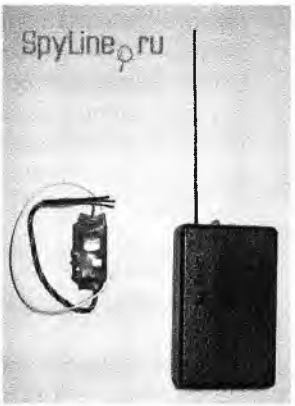
Для автоматической записи телефонных переговоров и регистрации входящих и исходящих звонков с помощью цифрового диктофона E-DIC LCD используется специальный адаптер. Он подключается к телефонной линии параллельно телефонному аппарату и к диктофону. С помощью специального программного обеспечения, идущего в комплекте с диктофоном, возможно настроить автоматическую запись переговоров.

**Функциональные особенности:**

- простота использования и установки;
- автоматическое включение и выключение (при поднятии и опускании трубки);
- фиксирует номер, дату, время звонков;
- определяет номера телефонов стандарта «Российский АОН»;
- высокое качество записи.

Производитель: Россия.

**Пульт для дистанционного включения/отключения радиомикрофонов**




Этот прибор предназначен для удаленного включения/отключения радиомикрофонов, что позволяет существенно экономить батареи и усложнить обнаружение радиомикрофона. Также, помимо управления беспроводными микрофонами или прослушкой, этим пультом дистанционного управления можно управлять многими приборами, питающимися от батареек, — машин на ДУ, лампами и т. д.

Режим работы пульта ДУ. При нажатии кнопки 1 на пульте ДУ включается ключ управления исполнительного модуля, подавая питание на выход 1 к нагрузке, и остается в этом режиме сколь угодно долго до получения команды выключения кнопкой 2. При этом напряжение питания на выходе 1 будет на 10% ниже питания, подаваемого на исполнительный модуль. Приемник исполнительного модуля все время находится в режиме сканирования, включаясь на 2 секунды через каждые 8 секунд. Кнопка 3 включает исполнительный модуль на 20 мин. В этом режиме приемник исполнительного модуля отключен, исполнительный модуль выключается.

**Тактико-технические характеристики:**
Дальность работы — до 200 метров.
Питание — пульт ДУ 9V (бат. «Крона»).
Исполнительный модуль от 3 – 9 вольт (батарейки или аккумуляторы).
Частота — 916 МГц.

## 3.3. Устройства несанкционированного съема аудиоинформации по GSM-каналу

### GSM-закладки

Это одно из последних решений в области GSM-прослушки. С помощью обычного мобильного телефона вы без труда сможете вести прослушивание разговоров, проводимых в радиусе действия GSM-передатчика. Устройство снабжено внутренней аккумуляторной батареей, а также возможностью подключить внешний элемент питания, значительно продлевая время автономной работы.

**Тактико-технические характеристики:**

Стандарт — 900/1800/1900 MHz.

Чувствительный микрофон позволяет отчетливо разбирать речь в радиусе 3 – 6 метров.

Время автономной работы в режиме ожидания / передачи / передачи с использованием внешней батареи — 240/3/6 часов.

Подключаем к бесперебойному источнику питания или компьютеру для постоянной работы.

Размеры — 56 × 35 × 13 мм.

**Комплектация:**

GSM-жучок — эффективная прослушка окружения телефона — 1 шт.

Сетевое зарядное устройство — 1 шт.

USB-кабель — 1 шт.

Внешняя батарея — 1 шт.


Подслушивающее устройство GSM осуществляет эффективную прослушку в качестве жучка, а передает информацию, как обычный сотовый телефон. Вы можете находиться рядом с устройством или на диаметрально противоположной стороне планеты и все равно осуществлять эффективную прослушку по телефону.

У новейшего беспроводного подслушивающего устройства GSM появились еще и новые удобные функции. Теперь вы сможете легко контролировать многие особенности в работе устройства с помощью СМС-сообщений. Например, узнать, каков баланс на счете вашего телефонного GSM-жучка или на какое время хватит заряда батареи такого беспроводного подслушивающего устройства.

**Тактико-технические характеристики:**

Питание — от сети или аккумуляторная батарея Li-Ion (1800 mA).

Автоматическая регулировка уровня входного сигнала.

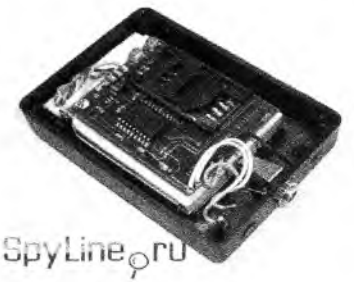
Защита от дозвона с посторонних номеров.

2 индикатора работы.

Возможность опрашивать состояние устройства с помощью СМС-команд.

Время работы в режиме ожидания — до 240 часов.

Время работы в режиме прослушки — до 250 минут (при 100% зарядке аккумулятора).




Стандарт передаваемого радиосигнала — GSM 900/1800.
Чувствительность микрофонного входа — до 11 метров.
Для полной зарядки аккумуляторной батареи необходимо 6 часов.
Вес — 78 г.
Размеры — 7×5,5×2,8 см.

**Комплектация:**

Усовершенствованное беспроводное прослушивающее GSM-устройство — 1 шт.

Сетевой адаптер (5V. 400 mA) — 1 шт.

**Программа для прослушивания SPS Audio Plus**

Программа SPS Audio Plus позволяет не только прослушивать окружение мобильного телефона, но и прослушивать разговор между абонентами GSM. Если вам, в силу обстоятельств, необходимо получить важную, но скрытую от вашего внимания информацию, данное программное решение будет идеальным.

SPY PHONE SUITE
audio plus

Сегодня трудно представить себе кого-либо без мобильного телефона. Действительно, этот аппарат, еще недавно описываемый лишь в фантастических романах, успел прочно войти в нашу жизнь. Что сегодня доверяют пользователи этому устройству? Все свои коммуникации, переписку короткими сообщениями, организацию свободного и рабочего времени, даже звонок будильника — и за это отвечает сотовый телефон.

GSM. Именно поэтому «прослушка» мобильного является самым эффективным способом контролировать «целевого абонента». Ведь, будучи незаметной, gsm-прослушка всегда, волей хозяина, будет рядом с ним, будет постоянно заряжаться и использоваться, давая вам возможность получения полной и объективной информации.

В течение 24 часов с момента зачисления средств вам приходит e-mail с программой и инструкцией по установке. Скачивание и установка программы для «прослушки» телефонов занимает менее 5 мин. Еще столько же настройка программы и ее активация. После чего можно спокойно отдавать новоиспеченное прослушивающее устройство. Затем у вас появляется возможность прослушивать окружение сотового (мобильника) абонента. Телефон при этом

начинает работать и как GSM-жучок. Если он лежит на столе и ведутся переговоры в радиусе 3—8 метров, то вы сможете стать полноправным слушателем беседы. При этом цифровые алгоритмы шумоподавления телефона, призванные оградить при телефонных разговорах от сторонних шумов, будут отключены, и вы будете отчетливо слышать даже тихие звуки вдали от сотового. В том случае, если вам необходимо узнать о предмете приватного разговора, то после минимальных настроек в программе на номер стороннего телефона будут посылаться скрытые СМС-уведомления о начале беседы, после чего вы беспрепятственно можете вклиниваться в разговор. Существует дополнительная технологическая возможность вести запись разговор интересующих вас абонентов, записывая их разговор на ПК. Специально для этого была создана программа для записи мобильных телефонных разговоров SPS RECORD, которая, помимо собственно записи разговора, щедро добавляет и другие полезные возможности.

Данный продукт позволяет легко и быстро узнать не только предмет разговоров «целевого абонента» по мобильному телефону, но и всего его окружения. Человек может тихо переговариваться в незнакомом месте, а лежащий рядом телефон любезно будет передавать голосовые данные заинтересованному кругу лиц. Также в программе реализовано СМС-уведомление о смене СИМ-карты целевого абонента и другие полезные решения.

| Функция/ Версия | | | | | |
|---|---|---|---|---|---|
| Прослушивание разговоров по сотовому телефону | | | | | |
| Использование телефона в качестве жучка | | | | | |
| Перехват СМС/ЕтаП/Журнала звонков | | | | | |
| Просмотр перехваченных данных через Интернет | | | | | |
| Отслеживание через GPS | | | | | |
| Уведомление о смене СИМ-карты | | | | | |

## 3.4. Устройства для несанкционированного съема видео- и аудиоинформации (УНСВАИ)

### Шпионская ручка

Данная шпионская ручка — это шариковая ручка со скрытой камерой высокого разрешения. Такая ручка с камерой внешне неотличима от обычной шариковой ручки. Эту ничем не примечательную

ручку очень удобно брать с собой, закрепив, например, в кармане пиджака.

В рабочем состоянии эта шпионская ручка незаметно записывает видео в разрешении 1280×960 точек и сохраняет материал в своей памяти, объем которой составляет целых 8 Гб. Вы можете купить такую ручку и использовать ее для записи переговоров, рабочих или личных встреч, ситуаций на дороге и прочих. Эта ручка с камерой способна не только записывать видео, но и делать фотоснимки. В любом случае, в котором только может понадобиться скрытая запись, вы сможете рассчитывать на такую шпионскую ручку со скрытой камерой.

При помощи такой ручки вы приобретете автономное записывающее устройство с действительно большим объемом памяти. Вы также можете использовать память такой шпионской ручки для хранения важных компьютерных файлов, как обычную флешку, объемом 8 Гб.

Разместите ручку-шпион в удобном для записи месте, и она будет фиксировать все, что происходит вокруг.

**Тактико-технические характеристики:**

Совместимые ОС: Windows ME / 2000 / XP / Vista / Windows7 / MAC OS X+.

Формат видеозаписи: AVI, 1280×960 точек, 30 кадров/сек.

Формат фотоизображений: JPEG, 1600×1200 точек.

Внутренняя память устройства: 8 Гб.

Встроенный микрофон.

Питание от встроенного аккумулятора.

Время работы в режиме записи — около 2 часов.

Зарядка устройства через USB-порт ПК.

Размеры: 14 мм×150 мм.

Функция автовключения при заданном уровне шума вокруг.

**Комплектация:**
Шпионская ручка 8 Гб с камерой высокого разрешения — 1 шт.
USB-кабель — 1 шт.
Автомобильное зарядное устройство — 1 шт.
Диск с ПО — 1 шт.

## Шпионские часы

**Тактико-технические характеристики:**
Внутренняя память — 2 Gb.
Встроенный микрофон.
Формат записываемых данных — AVI (352×288).
Рекомендуемое расстояние до объекта — 3 – 7 метров (для записи звука — 1 – 4 метра).
Питание — аккумуляторная батарея Li-ion.
Зарядка аккумулятора — через USB-порт или сетевой адаптер (110 – 240V 50/60Hz).
Аналоговый дисплей.
Материал — металл, стекло.
Светодиодный индикатор.
Совместимость: Windows 98SE / ME / 2000 / XP / Vista.
Размеры: 5×5×1,5 см.
Удобное включение/выключение камеры.
Непрерывная запись до остановки или до окончания свободной памяти.
**Комплектация:**
Шпионские часы со встроенной камерой слежения — 1 шт.
Сетевой адаптер (110 – 240V 50/60Hz) — 1 шт.
USB-кабель — 1 шт.
Диск с ПО — 1 шт.
Инструкция по эксплуатации — 1 шт.

### Миниатюрная камера в виде пуговицы

с устройством записи изображения. Вы можете записывать информацию на встроенные 1 GB памяти или дополнительно вставить карты формата SD/MMC. Также устройство записи можно использовать как проигрыватель МП-4 файлов.

### Беспроводная радиовидеокамера в виде солнцезащитных очков

и внешне ничем не отличается от обычной спортивной модели, что очень удобно и безопасно для скрытой видеосъемки. Она может быть как проводной, так и беспроводной. В маленькой оправе очков встроены: цветная видеокамера, микрофон, перезаряжаемый аккумулятор и передатчик.

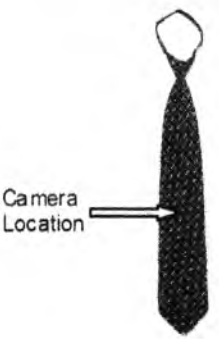
### Новая беспроводная видеокамера слежения в корпусе ID-карты (ID CARD)


позволит вам записывать разговоры и видеоизображение прямо на встроенную память беспроводной камеры видеонаблюдения. Беспроводная скрытая камера наблюдения может быть оформлена под ваш личный пропуск для прохода на интересующий вас объект и не будет привлекать внимание. С помощью скрытой видеокамеры вы также сможете делать фотографии.

### Беспроводная радиовидеокамера в виде обычной стирательной резинки

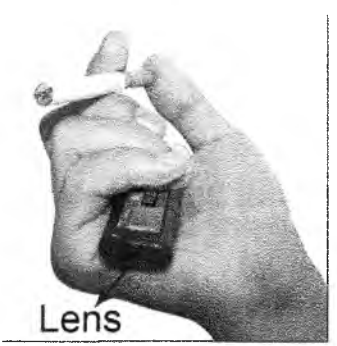

и с виду ничем от нее не отличается, что очень удобно и безопасно для скрытой видеосъемки. Она является полностью беспроводной и в маленьком корпусе стирательной резинки встроены: цветная видеокамера, микрофон, перезаряжаемый аккумулятор и 2,4 Ghz передатчик с антенной.

### Уникальная система скрытого видеонаблюдения, спрятана в классическом галстуке




Этот продукт представляет отличное решение для журналистов, бизнесменов, частных детективов и тех, кому по роду деятельности приходится производить съемку в условиях полной секретности. Камера расположена на идеальной для видеосъемки высоте. Довольно широкий угол обзора, микрофон высокой чувствительности и прекрасная передача изображения. Запись сигнала производится на встроенную память емкостью 4Гб. Включение записи происходит с помощью миниатюрного пульта управления. Время беспрерывной записи на карту 4 Гб до 280 минут.

### Видеокамера в зажигалке




С виду это обычная дешевая зажигалка, купленная в табачке, но это далеко не так. Внутри скрыто многофункциональное устройство, сочетающее в себе видеокамеру, фотоаппарат и диктофон. Несмотря на скромные габариты, технические характеристики и возможности впечатляющие; видео с разрешением 1280×960 и скоростью 30 кадров в секунду, фотоснимки также с разрешением 1280×960, матрица 2 мегапикселя. Устройство также имеет встроенный диктофон, аналогичный специализированным цифровым диктофонам, и оснащен детектором звука, осуществляющим запись только в моменты, сопровождающиеся каким-либо звуком.

### Видеокамера вмонтирована в брелок

Брелок, в который вмонтирована незаметная пинхольная камера и микрофон, которая записывает аудио-видео и делает фото высокого разрешения HD — всего, что вы захотите, при этом этого никто даже и не подозревает.

### Видеокамеры в игрушках

### Игрушечный радиоуправляемый автомобиль

со встроенной скрытой видеокамерой и системой удаленного управления. Вы можете следить за тем, куда направляется ваша радиоуправляемая машина, и за тем, что происходит вокруг нее, через ЖК-дисплей, расположенный на пульте дистанционного управления, благодаря встроенной скрытой камере слежения.

### Модель вертолета,


оборудованная камерой наблюдения, которая по радиоканалу передает изображение на видеорегистратор и позволяет не только наблюдать за определенными событиями, но и вести их запись.

### Суперминиатюрная видеокамера

Полностью беспроводная цветная суперминиатюрная видеокамера с передачей звука на расстояние до 100 м! Камера размером не более ногтя (25×20×21 мм), спокойно помещается в спичечный коробок, станет вашим верным другом и спутником для организации различных шпионских штучек и прочее. Возможность работы от «Кроны» до 5 часов. Камера также может работать и от входящего в комплект адаптера от 220 вольт неограниченное время.

## 3.5. Кейлоггеры

### Эксклюзивный аппаратный кейлоггер USB


Этот клавиатурный шпион — аппаратный кейлоггер может быть использован для многих целей. К примеру, кейлоггер можно использовать как взломщика для воровства паролей и любой другой секретной информации, вводимой с клавиатуры. Но аппаратный кейлоггер может быть также использован для слежки за детьми с целью узнать, чем занимается за компьютером ваш ребенок в ваше отсутствие. Также клавиатурный шпион может использоваться для оценки качества работы сотрудников офиса или для слежения за доступом к вашему рабочему компьютеру во время вашего отсутствия на рабочем месте. Данный клавиатурный шпион не может быть обнаружен программными средствами, поскольку «физически» находится вне зоны действия любой операционной системы. Именно поэтому наш клавиатурный шпион выгодно отличается от тех, что надо скачивать. Кейлоггер очень удобен в использовании благодаря USB-интерфейсу. Также этот аппаратный кейлоггер может быть использован просто как usb-накопитель для хранения информации.

**Тактико-технические характеристики:**
Встроенная память — 3 Mb.
Работает от USB-порта.
Не требует дополнительного питания.
Данные без потерь переносятся с одного ПК на другой.
Работает под любой операционной системой.
Не распознаваем антивирусами.
Клавиатурный шпион не надо дорабатывать скачиваниями и инсталляциями. Готов к применению сразу.

### Устройство для слежения за компьютером через Интернет


При помощи этого устройства слежения, установив с него специальную программу на любой компьютер, вы можете следить со своего ПК за тем, что происходит на ПК интересующего вас человека. При помощи скриншота рабочего стола вы можете посмотреть, чем в данный момент за-

нимается за своим ПК этот человек. Также вы при помощи установленной программы для слежения за компьютером можете ограничить доступ в Интернет (или время доступа в Интернет) или запретить вход на определенные сайты. Кроме того, вы сможете отслеживать все логи с интересующего ПК и знать, с кем и о чем говорит человек.

**Тактико-технические характеристики:**

Установка ПО для просмотра ПК в течение 60 секунд.
Возможность доступа к просматриваемому ПК с любого места, где есть Интернет.
Сохранение картинки рабочего стола (ScreenShot) просматриваемого ПК в любое время.
Просмотр списка посещенных сайтов.
Совместимость со всеми браузерами и Веб-приложениями.
Совместимость со всеми популярными IM-программами.
Автоматическая расшифровка наиболее часто употребляемых выражений в IM (таких как IMHO, LOL и т. д.).
Просмотр всех E-Mail протоколов (SMTP, POP3, IMAP) с целью получения информации об отправленной и полученной почте.
Возможность просмотра действий на ПК в режиме реального времени.
Возможность ведения history несмотря на то, пользуетесь ли вы режимом просмотра в реальном времени или нет.
Сохранение history прямо на внутреннюю память устройства.
Возможность хранения history на устройстве в течение 12 месяцев.
Все модули программы обновляются автоматически, поэтому вы имеете всегда последнюю версию ПО.
Возможность посылать пользователю предупреждающие сообщения.
Включения/выключения доступа в Интернет напрямую или удаленно.
Установка разрешенного времени для работы в Интернете.
Блокирование определенных программ, работающих через Интернет.
Блокирование определенных сайтов и портов на ПК.
Блокирование доступа к социальным сетям, таким как vkontakte.ru.
Полная защищенность. Только ваше устройство сможет получить доступ к вашему ПК или изменить настройки.
ОС — Windows 2000/XP/2003/Vista.
Внутренняя память — 256 Мб.

Наличие в памяти словаря наиболее часто используемых в Интернете сокращений.
Возможность просмотра до трех ПК одновременно.
Устройство подключается к компьютеру только на момент установки программного обеспечения.

### Кейлоггер, невидимый для операционных систем


Это уникальное устройство — кейлоггер не требует ни дополнительного питания, ни инсталляции программного обеспечения. Оно абсолютно невидимо для любой ОС. Установка занимает меньше минуты — просто установите его как переходник между клавиатурой и портом Ps/2, куда она подключается. После этого устройство начнет записывать все набранные с клавиатуры символы — начиная от поисковых запросов в сети, переписки с друзьями и заканчивая паролями, а также важными документами и секретными данными. Устройство имеет флэш-память 2 Mb, позволяя записать более миллиона символов, а это примерно полгода нормальной работы за ПК. Устройство не может быть обнаружено программными средствами, поскольку «физически» находится вне зоны действия любой операционной системы. Также невозможно обнаружить никаким детектором для жучков, поскольку устройство не излучает никаких сигналов. Единственный способ вывести информацию — это ввести специальный код, который активизирует шпиона, выводящий программу по поиску и просмотру текста, а также опции для работы с ним.

**Основные сферы применения**

Мониторинг за детьми, использующими ПК и Интернет. Оценка качества работы сотрудников компании в рабочее время. Слежение за несанкционированным доступом к вашему ПК. Хранение важных документов на случай потери данных на жестком диске.

**Тактико-технические характеристики**

Встроенная память — 2 mb.
Возможность использования на любом ПК, снабженном ps/2 портом.
Не требует дополнительного питания.
Данные без потерь переносятся с одного ПК на другой.

## 3.6. Устройства для GPS-слежения за местоположением объекта

### Устройство для спутникового мониторинга местоположения автомобиля


Устройство для спутникового мониторинга местоположения автомобиля с его отображением в графическом виде на экране смартфона или ПК. Если вы дорожите своим автомобилем, то вам стоит задуматься над тем, чтобы купить авто GPS-модуль — устройство GPS-слежения.

В отличие от большинства подобных авто GPS-систем, данное GPS-устройство имеет особый режим «Стелс», находясь в котором этот авто GPS способен работать без подключения к бортовой сети автомобиля до 300 суток. Это значительно снижает возможность его физического обнаружения автоугонщиками.

Другой важной особенностью данного авто GPS-устройства является то, что исключается возможность обнаружения сканером угонщика системы спутникового мониторинга, так как система не производит абсолютно никаких излучений до момента выхода в эфир. Обнаружить такое устройство авто GPS-слежения, таким образом, возможно лишь в течение 2 — 10 минут в сутки, в моменты передачи информации в режиме «Стелс». Эти уникальные особенности данного устройства делают этот прибор одним из лучших GPS-модулей, которые можно купить на сегодняшний день.

Управлять таким авто GPS-устройством вы можете дистанционно посредством СМС-команд. Также реализована возможность дистанционного управления внешним устройством, подключенным к данному устройству GPS-слежения. При помощи СМС-команд вы можете, например, блокировать двигатель автомобиля или включить сирену сигнализации. Контроль над вашим автомобилем и полная безопасность — вот что вы приобретете, купив данный GPS-модуль.

**Тактико-технические характеристики:**

Контроль местонахождения объекта по GPRS-каналу.
Отправка координат СМС-сообщением на указанный номер.
Отсутствие абонентской платы.
Работа системы без Интернета и промежуточного сервера.
Возможность записи координат на внутреннюю память.

Наличие датчика движения.
Точность определения местоположения: 3 м.
Точность определения скорости: 0,1 м/сек.
Вход сигнала «тревога».
Выход для управления внешним устройством до 300 мА.
Питание:
- внешнее от бортовой сети автомобиля 12 В;
- резервное от встроенного аккумулятора 1800 мАч.

Время работы от аккумулятора:
от суток в активном режиме до 300 суток в режиме «Стелс» (режим записи координат в память трекера, передача по запросу).
Размеры: 55 мм × 36 мм × 14 мм.

## Устройство для GPS-слежения – часы

В последнее время устройства для GPS-слежения принимают различные формы: это могут быть обычные GPS-трекеры, мобильные телефоны с GPS-модулем, замаскированные трекеры и прочие. Мы представляем вашему вниманию наручные часы с GPS, которые сочетают в себе все лучшие качества привычных GPS-трекеров с удобством наручных часов.

Используя технологию GPS-слежения, любой пользователь наручных часов с GPS-получает возможность определять свое местонахождение по всей планете, находить лучшие маршруты до заданной точки и многое другое. На циферблате наручных часов с GPS-находятся 8 светодиодов, которые выступают в роли своеобразного спутникового компаса. Эти светодиоды указывают направление искомого места на циферблате наручных часов с GPS-трекером, а их цвет и яркость помогут определить расстояние до цели.

Вы с легкостью можете разыскать, например, место, где оставили свой автомобиль. Для этого, выходя из машины, нужно нажать не только клавишу брелка сигнализации, но и специальную кнопку на корпусе нашего необычного устройства для GPS-слежения. Наручные часы с GPS-трекером запомнят координаты объекта и напомнят вам, где находится ваш автомобиль, даже если вы среди шумного бразильского карнавала.

Это устройство для GPS-слежения имеет возможность синхронизации с ПК.

Зарядка и передача информации из памяти наручных часов с GPS-трекером в память компьютера происходят через USB-порт. Это устройство для GPS-слежения обладает также несколькими дополнительными полезными и приятными функциями для активных пользователей Интернета, блоггеров и пользователей социальных сетей: это возможность работы напрямую с картами Google, размещать свои фотографии на Flickr с указанием точного места, где они были сделаны. Это понравится активным туристам.

**Тактико-технические характеристики:**

- 8 светодиодов для индикации направления.
- Возможность синхронизации с ПК и подзарядки батарей через USB-порт.
- Питание: встроенный литиевый аккумулятор на 800 мАч.
- Работа от одной подзарядки аккумулятора до 21 часа.
- Условия хранения и работы:
- рабочая температура от −20° до +60°C;
- температура хранения от −20° до +80°C.
- Возможность фиксации координат интересных вам мест.
- Возможность переключения между режимами определения местонахождения и фиксацией маршрута.
- Рабочая частота L1, 1575,42 МГц.
- Точность GPS-слежения: горизонтальное положение 10 м.
- Продолжительность процесса определения 1 миллисекунда.
- Условия для эффективного действия:
- максимальное ускорение: до 4 G;
- максимальная высота: до 18 000 метров;
- максимальная скорость: до 515 м/сек.
- Интервал фиксации местонахождения: по времени (от 1 сек до 30 мин) или расстоянию (от 1 до 65,535 метра).
- Объем памяти: до 100,000 записей во встроенной памяти — 8 Мбайт.
- Размеры: 45 мм × 18 мм.
- Влажность: до 95%.
- Интерфейс: USB-порт.
- Цвет: черный.

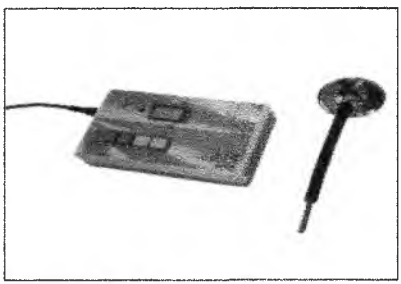
## 3.7. Электронные стетоскопы

**Тактико-технические характеристики**

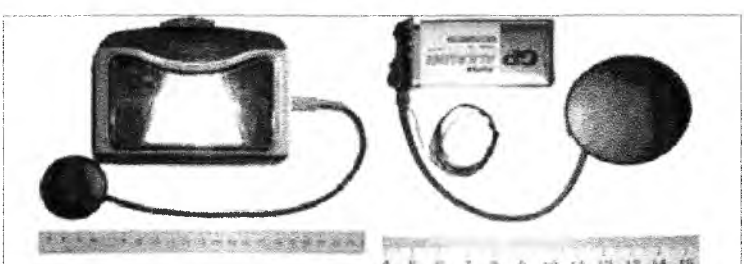
Удобное крепление на одежду.

Специальная технология для шумоподавления.

Высокочувствительный звуковой сенсор.
Специальный наушник для прослушивания.
Размеры: 7 × 4 × 1,8 см.
Вес: 36 г.

## Прослушивающие устройства, позволяющие вести контроль через стены, оконные рамы, коммуникационные трубы



| | |
|---|---|
| *Микрофон стетоскоп МС-01 Стены до 0,6 м сквозь тройной стеклопакет. Коэффициент усиления: 40 000* | *Беспроводной радиостетоскоп МС-02 Стены до 0,8 м. Время работы минимум 2 суток. Дальность до 700 м* |

Стетоскопы — это приборы, позволяющие подслушать через стены, окна или коммуникационные трубы. Стены, стекла и даже батареи замечательно передают разговор. Вибродатчик, закрепленный в смежном помещении или даже на улице, преобразует микровибрации в звук.

Стетоскопы могут быть оснащены радиопередатчиком, что дает возможность слушать и записывать разговор на значительном удалении.

### Радиостетоскоп МС2

Радиостетоскоп МС2 предназначен для прослушивания разговоров через стены (без захода в прослушиваемое помещение) из различных материалов толщиной до 0,8 метра и оконные рамы с двойными стеклами (материал не имеет значения). Подсоединение устройства к водопроводной трубе или к трубе отопительной системы позволяет свободно прослушивать разговоры в соседних помещениях с передачей акустической информации по радиоканалу и прослушивания на любом FM-приемнике. Радиостетоскоп МС2 состоит из двух блоков:

1. Вибрационный датчик с высокой чувствительностью, который крепится на плоскости с помощью двустороннего скотча либо специального клея.
2. Передающий модуль — усилитель для беспроводной передачи акустической информации. Прибор имеет встроенный фильтр частот — для лучшей разборчивости речи. Частота передающего модуля регулируется в диапазоне 96 – 108 Мгц.

**Технические характеристики:**

Максимальная дальность действия в условиях прямой видимости — 700 м.
Ток потребления — 16 мА.
Питание — 9 В.
Габариты передатчика (мм): 30 × 12 × 8.
Габариты датчика (мм): 50 × 20.
Температурный диапазон: от – 10 °С до + 40 °С.
Рабочая частота (МГц): 96 – 108 (регулируемая).
Источник питания: один элемент Alkaline.

Battery типа «Крона» 9 В.
Время работы от одного элемента питания:
— минимум двое суток;
— максимум зависит от типа и качества элемента питания.

## 3.8. Направленные микрофоны

В основном используются три вида направленных микрофонов: параболические (рефлекторные), трубчатые (интерференционные) и плоские микрофонные решетки.

### Направленный микрофон «Супер Ухо-100»

Наиболее простым по конструкции является направленный микрофон «Супер Ухо-100» (фото 1).

Параболический отражатель выполнен из пластика. В фокусе отражателя помещен электретный микрофон, подключенный к входу малошумящего усилителя низкой частоты. Встроенный 8-кратный бинокль позволяет точно навести микрофон на цель. Микрофон имеет размеры 290 × 150 × 90 мм и массу 1,2 кг. Питание микрофона осуществляется от батарейки типа «Крона». Время работы от внутренней батарейки — до 60 ч.

*Фото 1.*
*Направленный микрофон «Супер Ухо-100»*

Прослушивание перехватываемых разговоров осуществляется с использованием наушников. Микрофон имеет встроенный диктофон, позволяющий осуществлять запись перехваченных разговоров.

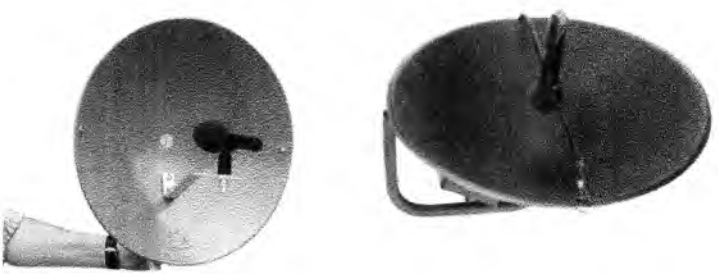


*Фото 2.*
*Внешний вид параболических направленных микрофонов*

*Фото 3.*
*Внешний вид параболических направленных микрофонов*

Диаграмма направленности микрофона — 10°, коэффициент усиления — 70 дБ, что обеспечивает перехват разговоров на открытой местности при низком уровне шума до 100 м. Частотный диапазон микрофона от 100 до 14000 Гц.

*Таблица 1*

**Основные характеристики направленных параболических микрофонов PKI2915 и PKI 2920**

| Характеристика | Тип микрофона | |
|---|---|---|
| | PKI2915 | PKI 2920 |
| Диаметр отражателя, м | 0,60 | 0,85 |
| Масса, кг | 0,38 | 0,40 |
| Дальность перехвата разговоров, м | 100 | 150 |
| Питание | Встроенный аккумулятор 9 В | |

*Таблица 2*

**Основные характеристики параболических микрофонов Super Sound Zoom и PR-1000**

| Характеристика | Тип микрофона | |
|---|---|---|
| | Super Sound Zoom | PR-1000 |
| Размеры, мм | 290 × 150 × 90 | 500 × 500 × 400 |
| Диапазон частот, кГц | 0,5 – 14 | 0,2 – 14 |
| Чувствительность, мВ/Па | 4 | 20 |
| Масса, кг | 1,2 | 1,5 |

*Таблица 3*

**Основные характеристики параболических микрофонов Spectra G50 и Big Ears BE3K**

| Характеристика | Тип микрофона | |
|---|---|---|
| | Spectra G50 | Big Ears BE3K |
| Размеры, мм | 500 × 500 × 400 | 750 × 750 × 400 |
| Диапазон частот, кГц | 0,1 – 15 | 0,1 – 15 |
| Чувствительность, мВ/Па | 31 | 50 |
| Масса, кг | 2 | 2,5 |

Дальность перехвата разговоров во многом зависит от диаметра отражателя. Например, для одних и тех же условий при диаметре отражателя 60 см (микрофон PKI 2915) дальность перехвата разговора составляет 100 м, а при диаметре 85 см (микрофон PKI 2920) — 150 м. Параболические микрофоны чаще всего маскируются под антенны спутникового телевидения и устанавливаются на балконах домов.

Микрофоны «бегущей волны» (интерференционные), часто называемые трубчатыми микрофонами, состоят из трубки с отверстиями или прорезями, на заднем торце которой расположен ненаправленный или однонаправленный микрофонный капсюль.

Трубчатые направленные микрофоны по сравнению с параболическими более компактные и используются в основном в случаях, когда необходимо обеспечить скрытность прослушивания разговоров. С использованием таких микрофонов разведку можно вести как из автомобиля, так и из окна расположенного напротив здания.

Внешний вид некоторых трубчатых микрофонов представлен на фото 4 – 7, а основные характеристики — в табл. 4, 5.

*Таблица 4*

**Характеристики направленных трубчатых микрофонов**

| **Характеристика** | **Тип микрофона** | | |
|---|---|---|---|
| | YKN | AT-89 | UEM-88 |
| Частотный диапазон, Гц | 500 – 10000 | 60 – 12000 | 200 – 15000 |
| Максимальный коэффициент усиления, дБ | 66 | 93 | 50 |
| Чувствительность, мВ/Па | 20 | 70 | – |
| Размеры, мм | 310 × 30 | 355 × 70 | 229 × 25 × 13 |
| Масса, г | 130 | 473 | 65 |
| Напряжение питания, В | 3 | 9 | 1 × AAA |
| Время работы от аккумулятора, ч | 30 | 4 – 6 | 100 |
| Дальность перехвата разговоров, м | 100 | 100 | – |

*Таблица 5*

**Характеристики трубчатых микрофонов**

| Характеристика | Тип микрофона | | | |
|---|---|---|---|---|
| | AT 4071A | MKH 70 P48 | KMR 82i | MFC800 |
| Диапазон частот, кГц | 0,03 – 20 | 0,05 – 20 | 0,02 – 20 | 0,02 – 20 |
| Чувствительность, мВ/Па | 89,1 | 50 | 21 | 18 |
| Размеры, мм | 395 × 21 × 21 | 410 × 25 × 25 | 395 × 21 × 21 | 500 × 25 × 250 |
| Масса, г | 155 | 180 | 250 | 350 |

***Фото 4. Внешний вид трубчатого направленного микрофона PKI 2925***

***Фото 5. Внешний вид трубчатого направленного микрофона YKN***

***Фото 6. Внешний вид трубчатого направленного микрофона Sennheiser MKH 70 P48***

***Фото 7. Миниатюрный направленный микрофон UEM-88***

К типовым трубчатым микрофонам относится направленный микрофон PKI 2925 (фото 4). Общая длина микрофона с трубкой 35 см составляет 85 см, масса — 525 г. Питание микрофона осуществляется от аккумуляторной батареи напряжением питания 3,6 В. Микрофон имеет встроенные фильтры высоких и низких частот.

Для ведения разведки используются и сверхминиатюрные микрофоны. Например, микрофон UEM-88 (фото 7) имеет размеры 229 × 25 × 13 мм и массу всего 65 г.

Предельная максимальная дальность действия трубчатых микрофонов несколько меньше, чем параболических. Но в условиях города их возможности практически одинаковы.

Так называемые «плоские» направленные микрофоны появились сравнительно недавно и представляют собой акустическую микрофонную решетку, включающую несколько десятков микрофонных капсюлей. Плоские микрофонные решетки также выпускаются в камуфлированном виде. Наиболее часто они камуфлируются под атташе-кейс, жилет или пояс.

*Фото 8. Микрофонная решетка фирмы G.R.A.S*

Внешний вид некоторых плоских микрофонов представлен на фото 8 – 10, а их основные характеристики — в табл. 6.

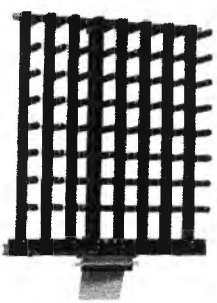


*Фото 9. Плоский направленный микрофон 40ТЛ*

*Фото 10. Микрофонная решетка BSWA-TECH SPS-980*

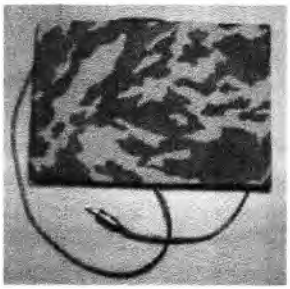
*Таблица 6*

**Плоский направленный микрофон 40ТЛ**

| Характеристика | Тип микрофона | |
|---|---|---|
| | 40ТА | SPS-980 |
| Количество микрофонов | 64 | 36 |
| Диапазон частот, кГц | 0,05 – 6,6 | 0,02 – 20 |
| Чувствительность, мВ/Па | 50 (4) | 50 |
| Динамический диапазон, дБА г | 32 (40) – 134 (174) | 30 – 128 |
| Размеры решетки, мм | 175 × 175 | 1000 |

Максимальная дальность действия направленных микрофонов в условиях города не превышает 100 – 150 м, за городом при низком уровне шумов дальность разведки может составлять до 500 м и более.

### Направленный микрофон А25



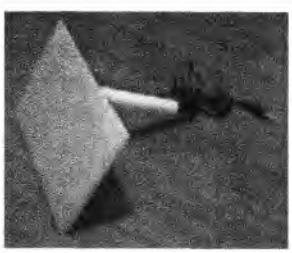
Направленный микрофон (НМ-А25) представляет собой плоскую фазированную микрофонную решетку с апертурой 25 см и коэффициентом усиления не менее 40 дБ.

**Основные ТТХ НМ-А25:**

Размеры 25×17×0,8 см; вес — около 0,3 кг; чувствительность — 0,3 В/Па; уровень приведенных собственных шумов — около 0 дБ; динамический диапазон — 110 дБ;

- эффективная ширина диаграммы направленности — не более 14°, при подавлении помех вне диаграммы не менее 20 дБ;
- оптимальные АЧХ для речевых сигналов и адаптивная обработка акустических сигналов;
- ветрозащищенность, обеспеченная конструкцией.

### Остронаправленный ветрозащищенный микрофон «ОВМ-01»



Направленный микрофон (ОВМ) представляет собой микрофонную фазированную решетку. Оптимальная схема согласования позволила получить высокую чувствительность и малый уровень приведенных собственных шумов при эффективной ветрозащите без воздушных отверстий. ОВМ обладает самой узкой диаграммой направленности из всех существующих микрофонов этого класса.

ОВМ может применяться для записи репортажей в условиях шумной улицы (60 – 70 дБА) на расстояниях до 10 м и на расстояниях 30 – 100 м, при уровне помех 40 – 20 дБА, эффективно поможет на охоте.

**Основные ТТХ РНМ-01:**

полоса рабочих частот — 0,1 – 7 кГц;
уровень собственных шумов — не более 0 дБ;
чувствительность — 100 мВ/Па × 3 дБ.
размеры 240 × 165 × 7 мм;
вес — около 150 г;
динамический диапазон — 110 дБ;
оптимальные АЧХ для речевых сигналов;
ветрозащищенность, обеспеченная конструкцией.

### Направленный микрофон «Суперухо плюс»

Направленный микрофон «Суперухо плюс» предназначен для улавливания и усиления звуковых сигналов вокруг вас, он делает их более легкими для прослушивания. «Суперухо плюс» является самым миниатюрным из своих предшественников, прибор удобен и легок в эксплуатации. Прибор стилизован под гарнитуру БлюТус и поэтому вам не составит труда быть незамеченным.

Благодаря своим небольшим размерам прибор легко поместится в кармане пиджака, рубашки и т. д., его можно брать с собой везде.

Одной из особенностей «Суперуха плюс» является то, что, в отличие от других направленных микрофонов, вам не нужно надевать наушники и направлять постоянно микрофон в сторону объекта, прибор фиксируется в ушной раковине с помощью специального ушного держателя, как левостороннего, так и правостороннего. Также «Суперухо плюс» стилизован под обычную беспроводную гарнитуру для мобильных телефонов и со стороны он неотличим от нее. Ушной держатель гибкий и эластичный, поэтому он хорошо фиксируется на ушной раковине любого размера, вдобавок ко всему у прибора есть ряд ушных насадок различного размера.

Питание прибора осуществляется от двух воздушно цинковых батарей 1,4 вольта, что обеспечивает работу усилителя звука приблизительно до 60 часов.

Включение и выключение прибора происходит с помощью регулятора громкости, при этом сразу же загорается синий индикатор на внешней стороне устройства.

**Технические характеристики**

Питание от двух батареек 1,4 В.

Диапазон рабочих температур от 0 до + 40 °С.

Тип корпуса — пластик.

Усиливает звуковые сигналы и речь примерно до 20 метров.

Габаритные размеры — 55 × 15 × 13 мм.

## 3.9. Лазерные акустические системы разведки

Если окна и форточки в выделенном помещении будут закрыты, прослушать разговоры, ведущиеся в нем, с использованием направленных микрофонов невозможно. Однако в этом случае возможно прослушивание разговоров с использованием лазерных акустических систем разведки (ЛАСР), иногда называемых «лазерными микрофонами».

Существуют несколько схем построения ЛАСР.

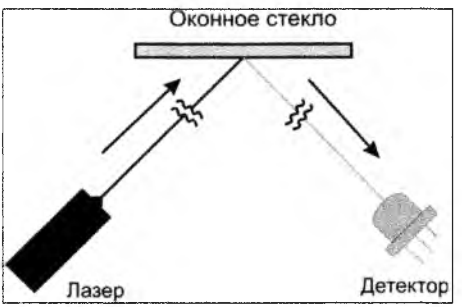



*Рис. 3.*
*Простейший вариант схемы построения ЛАСР*

На рис. 3 изображен простейший вариант подобной системы. Луч лазера падает на стекло окна под некоторым углом. На границе стекло – воздух происходит модуляция луча звуковыми колебаниями. Отраженный луч улавливается фотодетектором, расположенным на оси отраженного луча, и осуществляется амплитудная демодуляция отраженного излучения. Система довольно простая, но требует тщательной юстировки и на практике используется довольно редко.

Второй способ, использующий сплиттер (делитель) пучка, несколько сложнее, но он позволяет совместить лазер и детектор (рис. 4). Отпадает необходимость в тщательной юстировке системы. Применение

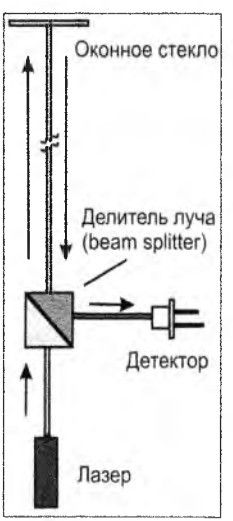



*Рис. 4.*
*Вариант схемы построения ЛАСР с использованием сплиттера (делителя) пучка*

сплиттера позволяет свести падающий и отраженный луч в одну точку.

В целях повышения чувствительности используется интерференционная схема, изображенная на рис. 5,а. Интерферометр, представленный на этом рисунке, имеет плечи равной длины и называется «Dual Beam LASER Mic».

Главный принцип этой схемы — дифференциальный метод измерения акустической вибрации. Участок оконного стекла, с которого снимается вибрация, имеет малый размер, следовательно, резко ослабляется синфазная помеха, вызываемая низкочастотными колебаниями стекла, например, из-за ветра или уличных шумов.

Приемник излучения может иметь свою оптическую систему, как показано на рис. 5, б.

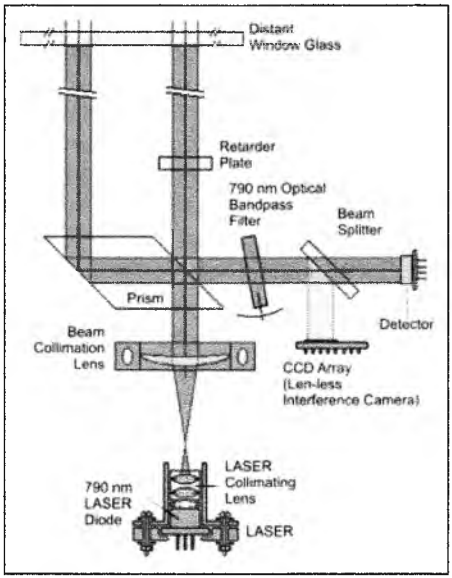
Принцип работы ЛАСР для систем с разделением луча (Single Split beam) можно представить следующим образом: когерентный луч лазера расщепляется разделительным стеклом (особое стекло со специальным покрытием толщиной в десятки нанометров пропускает 50 % и отражает 50 % света определенной длины волны) на две части: опорный луч и излучаемый. При отражении излучаемого луча от оконного стекла или триппель-призмы, установленной на нем, происходит его модуляция звуковой частотой. Отраженный промодулированный луч направляется на фоторезистор, где интерферирует с опорным лучом. Сигнал с фоторезистора после специальной обработки усиливается и подается для прослушивания на головные телефоны или записывается на цифровой диктофон.

Применение последних интерференционных схем возможно только в том случае, если луч лазера отражается в направлении его источника. А это возможно, если ЛАСР и облучаемое окно находятся на одной высоте и оконное стекло расположено перпендикулярно лучу лазера или на оконном стекле установлена триппель-призма. Во всех остальных случаях в направлении на детектор отражается незначительное количество диффузно рассеянного излучения и дальность ведения разведки резко снижается.

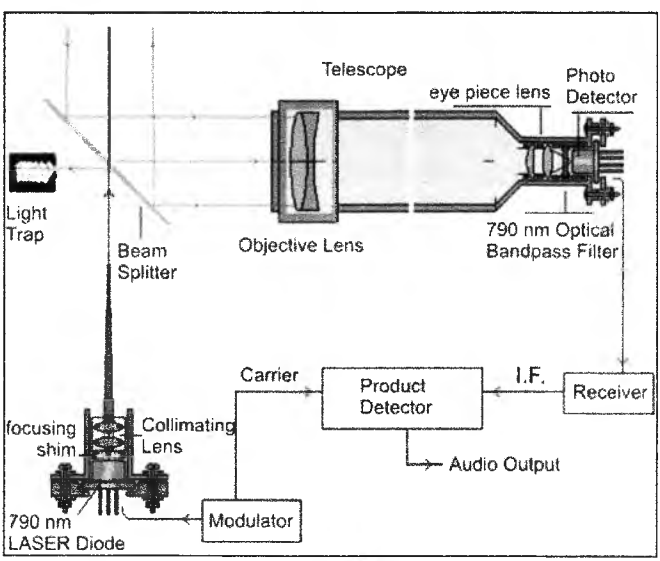
В целях обеспечения скрытности работы в ЛАСР используются лазеры, работающие в ближнем инфракрасном, не видимом глазу диапазоне длин волн (0,75 – 1,1 мкм).

Внешний вид некоторых ЛАСР приведен на фото 11 – 13, а их характеристики — в табл. 7, 8.

К типовой лазерной акустической системе разведки относится система SIM – LAMIC (фото 11), которая состоит из передатчика на основе полупроводникового лазера мощностью 5 мВт, работающего в диапазоне 0,82 мкм (фокусное расстояние объектива 135 мм), и при-




*а)*



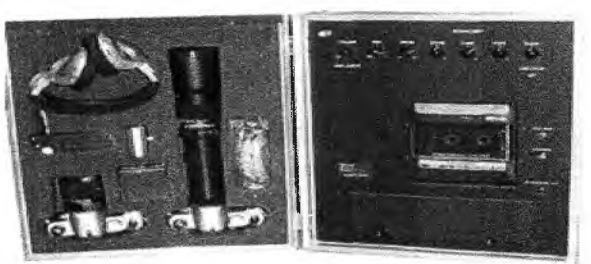

*б)*

*Рис. 5.*
*Простейший вариант схемы построения ЛАСР*

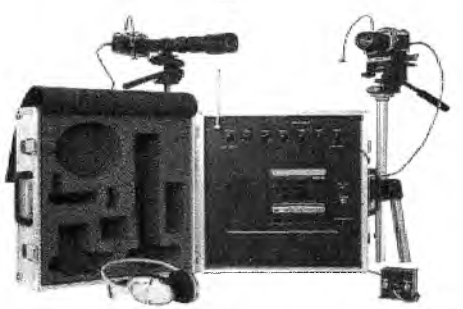
емника лазерного излучения на основе малошумящего PIN-диода (фокусное расстояние объектива 500 мм), закамуфлированного под стандартную зеркальную камеру. Передатчик и приемник устанавливаются на специальных треногах. При переноске вся система размещается в обычном кейсе. Аналогичная система, но работающая в диапазоне длин волн от 1,75 – 1,84 мкм, представлена на фото 12.

В системе PKI 3100 [6, 10] в отличие от SIM – LAMIC лазер и приемник оптического излучения размещены в одном приемо-передающем блоке (модуле) (фото 13). Мощность лазера 10 мВт, длина излучения 0,88 мкм, расходимость луча лазера 0,5 мрад. При такой расходимости размер пятна лазерного излучения на расстоянии 100 м составит 5 см.

Дальность действия лазерных акустических систем разведки при приеме диффузно отраженного излучения не превышает нескольких десятков метров. При приеме зеркально отраженного луча дальность разведки может составлять несколько сот метров, а при использовании триппель-призм она может превышать 500 м.



*а)*



*б)*

*Фото 11.*
*Лазерная акустическая система разведки SIM–LAMIC: а – упакованная в кейсе; б – в развернутом состоянии*

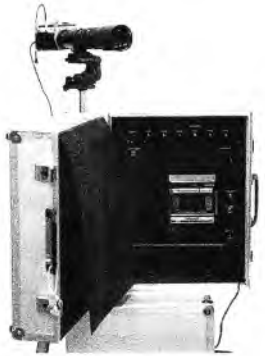


*Фото 12.*
*Лазерная акустическая система разведки Laser-3500*

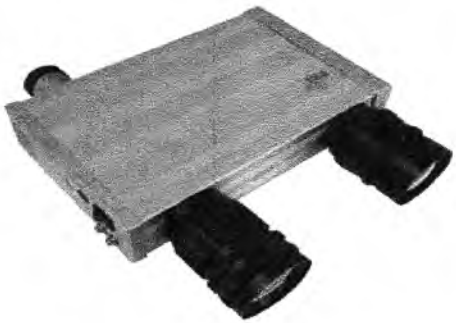


*Фото 13.*
*Лазерная акустическая система разведки PKI 3100 (приемо-передающий блок)*

*Таблица 7*

**Основные характеристики лазерных акустических систем разведки**

| Характеристика | Тип системы | |
|---|---|---|
| | SIM – LAMIC | Laser-3000 (PKI3100) |
| Лазерный передатчик | | |
| Тип лазера | Полупроводниковый | |
| Длина волны, мкм | 0,82 | 0,88 |
| Мощность излучения, мВт | 5 | 10 |
| Расходимость луча, мрад | – | 0,5 |
| Фокусное расстояние объектива, мм | 135 | 135 |
| Питание, В | 8×1,5 (AA) | 4×1,5 (AA) |
| Время работы, ч | 50 | 50 |
| Приемник лазерного излучения | | |
| Тип приемника | малошумящий PIN-диод | |
| Длина волны, мкм | ближний ПК | |
| Фокусное расстояние объектива, мм | 500 | 135 (1:2,8) |
| Питание, В | 12 | 4×1,5 (AA) |
| Время работы, ч | 50 – 100 | 50 |

| | | |
|---|---|---|
| Примечание | камуфлируется под стандартную зеркальную камеру; передатчик и приемник устанавливаются на треноге; не требует юстировки | размеры приемо-передающего блока 130 × 220 × 60 мм; масса 1,6 кг; усилительный блок (коэффициент усиления: 100 дБ; эквалайзер: 300, 600, 1200, 2400, 4800 Гц; диапазон регулировки 10 дБ; размеры 250 × 280 × 50 мм; масса 8,2 кг) |

*Таблица 8*

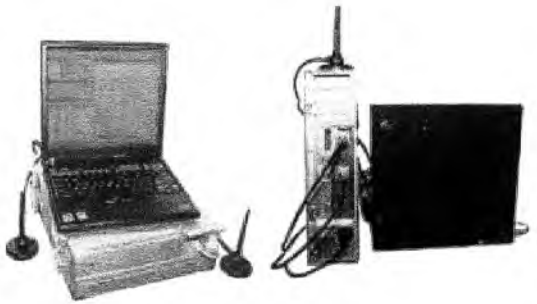
**Основные характеристики лазерных акустических систем разведки**

| Характеристика | Тип системы | | |
|---|---|---|---|
| | LASR-2000 | Laser-3500 | MR-7800 |
| Лазерный передатчик | | | |
| Тип лазера | полупроводниковый | | |
| Длина волны, мкм | 0,75 – 0,84 | 1,75 – 1,84 | 0,77 – 0,84 |
| Мощность излучения, мВт | 5 | 5 | 25 |
| Фокусное расстояние объектива, мм | 135 | 135 | 135 |
| Питание, В | 8 × 1,5 (АА) | 8 × 1,5 (АА) | 8 × 1,5 (АА) |
| Время работы, ч | 50 | 40 | 40 |
| Приемник лазерного излучения | | | |
| Тип приемника | малошумящий PIN-диод; ближний ПК | | |
| Фокусное расстояние объектива, мм | 500 | 500 | 500 |
| Питание, В | 9 | 12 | 12 |
| Время работы, ч | 15 – 30 | 15 – 50 | 40 – 60 |
| Примечание | камуфлируется под стандартную зеркальную камеру; габариты 470 × 380 × 220 мм; масса 10,5 кг без батарей и треног | | |

## 3.10. Системы прослушивания GSM-телефонов

### GSS-ProA – Система перехвата GSM

Система GSS-ProA — самая лучшая система перехвата и прослушивания GSM непосредственно с радиоэфира из всех доступных в мире на настоящий момент. Ни одна пассивная система перехвата не обладает такими возможностями для перехвата и прослушивания. Система абсолютно невидима и не поддается обнаружению,



обладает высокой производительностью, имеет возможность дальнейшей модернизации, многоканальный перехват сотовых телефонов и записи как информации о разговорах, так и самих разговоров. Система представляет собой не только устройство для перехвата и прослушивания сигналов сети GSM, но также имеет встроенный сложный RF-локатор, по методу триангуляции определяющий местоположение объекта с точностью до нескольких метров, близкой к GPS.

Система GSS-ProA способна перехватывать разговоры по GSM-телефонам по всему миру в сетях 900/1800/1900 МГц. Она перехватывает одновременно сигнал базовой станции и мобильной станции независимо друг от друга. Автоматически или вручную системой будет произведена запись разговора между двумя телефонами объектов одновременно, а разговор будет сохранен в виде стандартного WAV-файла.

**Особенности:**

Полностью пассивный (не поддающийся обнаружению) перехват GSM-переговоров с эфира.

Перехват и прослушивание зашифрованных голосовых каналов с алгоритмами A5.1, A5.2, A5.3.

Извлечение ключа Ki (Захват Ki) из эфира на расстоянии до 4 миль. Новая возможность!

Все действия выполняются незаметно для телефона объекта прослушивания и оператора сети сотовой связи GSM.

Автоматически перехватывает звонки к/от объекта, находящегося в специальном списке.

Перехват и прослушивание звонков, сделанных за границу. Новая возможность!

Базовая версия поддерживает 4 полнодуплексных канала. Это означает, что одновременно можно прослушивать до 4 телефонов одновременно.

Перехват SMS, факса и E-mail. Новая возможность!

Встроенная система определения местоположения даже внутри зданий с точностью до нескольких метров, аналогичная GPS. Новая возможность!

Встроенная система распознавания голоса (военная технология RF-триангуляции).

Автоматическое или ручное сканирование диапазона частот каналов на наличие активных соединений.

Установка рабочих режимов и параметров отслеживания.

Авто- или ручное изменение параметров отслеживания сигнала от базовой станции до абонента.

Сохранение настроек на жесткий диск с возможностью их последующей загрузки.

Запись разговоров на жесткий диск или внешний носитель.

Автоматическое отслеживание объектов из списка.

Возможность прослушивания и записи переговоров в реальном времени.

Возможность поддерживать и отображать протоколы передач данных на базовых станциях, а также информацию об отслеживаемых абонентах.

Отображение текущего состояния принимающих каналов (присутствие синхронизации, уровень и сила сигнала, активность во временных слотах).

Типичный радиус зоны отслеживания 1—5 км при использовании улучшенных антенн.

Устройство автоматически подключится к сотовому телефону объекта, как только он начнет разговор, сразу после внесения в базу следующих номеров:

*a.* ***TMSI*** (временный международный идентификационный номер пользователя).

*b.* ***IMSA*** (международный идентификационный номер абонента).

*c.* ***IMEI*** (международный идентификатор мобильного оборудования). В системе может быть записано до 700 000 номеров с присвоением им различного приоритета. Система работает как в незашифрованной, так и в зашифрованной сети GSM, независимо от сотового оператора. Точное определение местоположения объекта

по сотовому телефону, в том числе внутри здания и на конкретном этаже.

С помощью специально разработанного программного обеспечения GSS-ProA позволяет оператору определять местоположение объекта слежения в международном масштабе. Это стало возможным за счет триангуляции местоположения сотового телефона относительно базовых станций. В городах, где находится большое количество базовых станций, точность составляет ± 2 метра. За городской чертой, где плотность расположения базовых станций меньше, точность составляет ± 100 — 250 метров.

**Функции управления:**

- Создание контрольной базы данных
- Создание базы данных голосовых каналов
- Занесение Ki в базу данных объектов (номер цели)
- Наблюдение и создание отчетов активности объектов
- Автоматическое или ручное управление и наблюдение
- Отслеживание включения голосовых каналов
- Связь с различными компьютерами по сети
- Анализ информации, проходящей по контролируемым каналам
- Сохранение звуковых файлов из звуковых каналов в процессе разговора
- Анализ информации, проходящей по голосовым каналам
- Обработка голосовых сигналов из голосовых каналов
- Контроль системы цифрового отслеживания разговоров и передачи данных

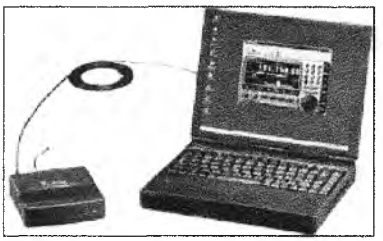
**Система GSS-ProA доступна в трех конфигурациях:**

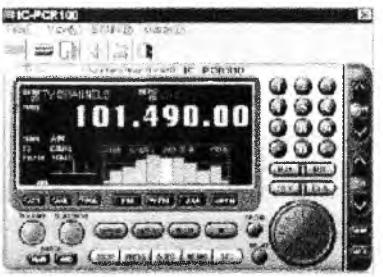
Портативное или стационарное 4-, 20- или 100-канальное устройство для полнодуплексного прослушивания разговоров по соответствующему количеству сотовых телефонов одновременно.

## 3.11. Сканеры

### Icom IC-PCR100 с компьютерным интерфейсом

ICOM IC-PCR100 — профессиональный связной сканер с широким набором специальных функций. Упрощение схемы входных фильтров и использование пластмассового корпуса позволило заметно снизить цену по сравнению с ICOM IC-PCR1000.






Расширенные возможности компьютерного интерфейса. Обмен осуществляется через последовательный порт в специально разработанном фирмой ICOM формате и позволяет как считывать данные (частоты, уровень сигнала), так и управлять всеми функциями приемника. Приемник выполнен в виде отдельного блока с независимым от компьютера питанием и управлением через последовательный порт. Шесть функций сканирования: диапазонное, по каналам памяти, по видам сигнала, по группам каналов памяти, приоритетное, с автоматической записью частот.

Расширенные объем и функции использования памяти. В каждом канале запоминается частота, вид модуляции (включая ширину полосы), шаг настройки и т. д. 1000 каналов памяти разбиты на 20 банков по 50 каналов. Каналам и банкам памяти можно присвоить буквенные имена.

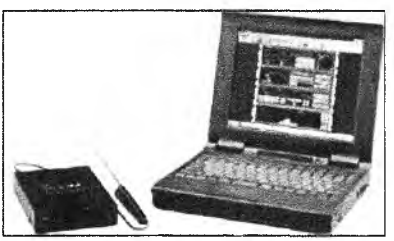
Удобство настройки. Предусмотрено два метода ввода частоты: с клавиатуры или с помощью «вращения» ручки настройки (управляемой мышью).

| **Технические характеристики** | **ICOM IC-PCR100** | | | |
|---|---|---|---|---|
| Диапазон частот, МГц | 0,01...1300 | | | |
| Виды модуляции | SSB, AM, CW, FM, WFI | | | M |
| Чувствительность, мкВ (AM при 10дБ S/N, FM, WFM при 12 дБ SINAD) | Диапазон, МГц | AM | FM | WFM |
| | 0,5...1,8 | 2,5 | – | – |
| | 1,8...28 | 1,8 | – | – |
| | 28...50 | 1,8 | 0,5 | – |
| | 50...700 | 1,0 | 0,32 | 0,79 |
| | 700...1300 | 1,3 | 0,4 | 1,0 |
| Количество каналов памяти | 1000/файл | | | |
| Диапазон рабочих температур | -0... + 50 °C | | | |
| Габариты и вес | 131 × 34 × 155 мм, 0,5 кг | | | |

### Icom IC-PCR1000 с компьютерным интерфейсом

ICOM IC-PCR1000 — это не просто приемник для компьютера, это профессиональный связной сканер с широким набором специальных функций — начиная от скоростного поиска сигналов и кончая развитым компьютерным интерфейсом.

Расширенные возможности компьютерного интерфейса. На задней панели приемника расположен последовательный порт для непосредственного подключения к компьютеру. Обмен осуществляется в специально разработанном фирмой ICOM формате и позволяет как считывать данные (частоты, уровень сигнала), так и управлять всеми функциями приемника. В отличие от большинства существующих компьютерных приемников, вставляемых в слот расширения материнской платы, фирма ICOM решила выполнить приемник в виде отдельного блока с независимым от компьютера питанием и управлением через последовательный порт. Это позволило решить две важные проблемы: уменьшить уровень шума и обеспечить совместимость с любым ПК.



Простота и удобство работы.

Широкий диапазон: 0,01 — 1300 МГц с шагом от 1Гц. Такой шаг перестройки частоты стал возможным благодаря новой разработке ICOM — системе DDS (Direct Digital Synthesizer).

Виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM, включая специальные виды: узкая CW (2,8 кГц), широкая и узкая AM (2,8/6/15/50 кГц), широкая и узкая FM (6/15/50/230 кГц).

Повышенное качество приема. Схема сдвига промежуточной частоты (IF shift) впервые встроена в приемник такого класса. Сдвиг ПЧ позволяет разделить близкорасположенные сигналы, что особенно эффективно при работе с CW или SSB. Качество приема повышается также за счет применения подавителя импульсных помех (Noise Blanker), ВЧ-аттенюатора (20дБ), автоматической регулировки усиления (АРУ) и подстройки частоты (АПЧ). Разработанный ICOM цифровой контур АПЧ позволяет полностью устранить уходы частоты в режиме FM даже при работе с фильтрами 6 или 15 кГц и заметно увеличивает стабильность приема на частотах выше 1000 МГц. Специальные перестраиваемые полосовые фильтры на частотах выше 50 МГц улучшают чувствительность и подавление зеркальных помех. Это позволяет также минимизировать искаже-

ния сигналов от близкорасположенных мощных передатчиков. Благодаря описанным выше схемным решениям чувствительность приемника в диапазоне от 28 до 1300 МГц практически не зависит от частоты и вида модуляции.

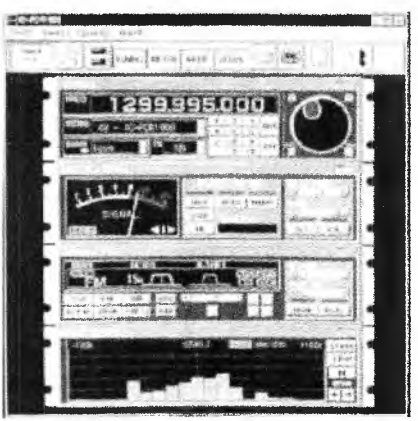
Программное обеспечение (на английском языке) входит в комплект поставки и включает три вида экранов (окон), отличающихся количеством органов управления и рассчитанных на пользователей с разным уровнем подготовки.

1. Окно упрощенной настройки — содержит индикатор частоты и кнопки фиксированных настроек (аналогично бытовому тюнеру).

2. Окно с изображением полной передней панели профессионального связного приемника — показывает частоту, силу сигнала (S-метр), ручку настройки, цифровую клавиатуру и т. д.

3. Окно с панелями дополнительных настроек — подробно показаны все органы управления, экран разделен на 4 секции (4 блока аппаратуры):

**Настройка (tuning)**
**Измерение/ сканирование (meter/scan)**
**Модуляция/ громкость (mode/vol)**
**Спектроскоп (bandscope)**




Спектроскоп. Очень удобно реализована функция спектроскопа, благодаря высокой скорости обмена (до 38 400) он практически работает в реальном времени. Максимальная полоса обзора составляет 200 кГц. Помещая курсор мыши на любую точку спектра, можно мгновенно перескочить на нужную частоту.

Расширенные объем и функции использования памяти. В каждом канале запоминается частота, вид модуляции (включая ширину полосы), шаг настройки и т. д. Для повышения эффективности память разделена на банки и на области автоматической записи или пропуска. Каналам и банкам памяти можно присвоить буквенные имена. Общее количество каналов не ограничено и зависит только от свободного пространства на диске. Встроенный редактор памяти позволяет легко производить копирование и вставку содержимого каналов.

6 типов сканирования: диапазонное, по каналам памяти, по видам сигнала, по группам каналов памяти, приоритетное, с автоматической записью частот. Скорость сканирования — до 50 каналов в секунду (как в режиме сканирования по каналам памяти, так и при программируемом сканировании). Время задержки также плавно регулируется. Интеллектуальная система поиска голоса. VSC (ICOM Voice Scan Control) позволяет пропускать модулированные и шумовые сигналы.

Удобство настройки. Предусмотрено два метода ввода частоты: с клавиатуры или с помощью вращения ручки настройки (управляемой мышью). Шаг настройки регулируется в пределах от 1Гц до 1МГц. Дополнительно существует режим программируемого шага, устанавливаемого индивидуально для каждого канала.

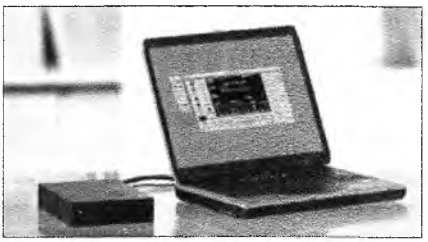
Декодирование тонов CTCSS и DTMF с возможностью выполнения действия (например, запуска программы) при приеме определенной DTMF последовательности.

| **Технические характеристики** | **ICOM IC-PCR1000** | | | | |
|---|---|---|---|---|---|
| Диапазон частот, МГц | 0.01...1300 | | | | |
| Виды модуляции | SSB, AM, CW, FM, WFM | | | | |
| Чувствительность, мкВ (AM, SSB, CW при 10дБ S/N, FM, WFM при 12 дБ SINAD) | Диапазон, МГц | FM | WFM | AM | SSB, CW |
| | 0.5...1.8 | – | – | 2.5 | 0.56 |
| | 1.8...28 | – | – | 1.4 | 0.28 |
| | 28...30 | 0.5 | – | 1.4 | 0.28 |
| | 30...50 | 0.5 | – | 1.8 | 0.35 |
| | 50...700 | 0.32 | 0.79 | 1.0 | 0.2 |
| | 700...1300 | 0.4 | 1.0 | 1.3 | 0.25 |
| Количество каналов памяти | Не ограничено | | | | |
| Потребляемый ток, мА | 0.7 (максимальная скорость) | | | | |
| Диапазон рабочих температур | −0°...+50 °C | | | | |
| Габариты и вес | 128×30×199 | | | | |

## Icom IC-PCR1500 с компьютерным интерфейсом

Компьютерный широкополосный сканирующий приемник.

IC-PCR1500 — это приемник с компьютерным управлением, всеми его функциями легко управлять при помощи мыши и клавиатуры. Охватывает диапазон частот от 0,01 до 3299,999 МГц с любым видом модуляции (в диапазоне от 0,495 до 1300 МГц работает только в режимах модуляции CW и SSB). Шаг перестройки 1 Гц, такой шаг перестройки частоты стал возможен благодаря разработке ICOM — системе DDS (Direct Digital Synthesizer).



Виды модуляции 1 SSB (USBF LSB), CWF AM, FM, WFMF, включая специальные виды: узкая CW (2,8 кГц), широкая и узкая AM (2,8/6/15/50 кГц), широкая и узкая FM (6/15 / 50 /230 кГц). Диапазон частот зависит от версии.

Соединение через USB-интерфейс. Для соединения с компьютером используется USB-интерфейс. Он обеспечивает большую скорость передачи данных, чем порт RS-232C, и позволяет оперативнее управлять приемником. Также он позволяет передавать полученный звуковой сигнал на подключенный компьютер и прослушивать или записывать его.

**Три вида управляющего интерфейса**

Рассчитаны на потребности пользователя или уровень подготовленности. Программное обеспечение (на английском языке) входит в комплект поставки и включает три вида экранов (окон), отличающихся количеством органов управления и рассчитанных на пользователей с разным уровнем подготовки.

1. Окно упрощенной настройки — содержит индикатор частоты и кнопки фиксированных настроек (аналогично бытовому тюнеру).
2. Окно с изображением полной передней панели профессионального связного приемника — показывает частоту, силу сигнала, ручку настройки, цифровую клавиатуру и т. д.
3. Окно с панелями дополнительных настроек — подробно показаны все органы управления, экран разделен на 4 секции (4 блока аппаратуры).

Неограниченное число каналов.

Каналы сохраняются на жестком диске компьютера или на другом запоминающем устройстве, таким образом, количество сохраненных каналов ограничивается только объемом свободной памяти.

**Функция многоканального мониторинга**

Эта функция позволяет быстро просматривать на экране состояние до 25 каналов из расчета силы принимаемого сигнала, активность канала индицируется на экране тремя различными фоновыми цветами. Простым нажатием на кнопку интересующего вас канала вы можете начать его прослушивание.

**Два вида спектроскопа**

IC-PCR1500 имеет функцию спектроскопа двух видов, позволяющую вам просматривать содержимое спектра определенной полосы частот (25 кГц — 5 МГц) либо просматривать временную диаграмму (от 3 до 100 минут). При сканировании диапазона звук выдается через звуковой выход. Когда вы обнаруживаете сигнал, который хотите прослушать, вы нажимаете на изображение спектра в нужном месте, после этого приемник настраивается на выбранную частоту. При сканировании данные спектроскопа могут быть сохранены на компьютере.

Звук не выдается в CW- и SSB-режимах модуляции, также звук не выдается при сканировании диапазона частот от 500 кГц до 5 МГц.

Быстрое сканирование — до 60 каналов в секунду.

Скорость сканирования IC-PCR1500 до 60 каналов в секунду предоставляет высочайшую эффективность поиска в широком частотном диапазоне. Автоматическое запоминание каналов при поиске. В режиме сканирования с автоматической записью частот происходит запоминание частот найденных сигналов в специальный банк памяти.

Типы сканирования: диапазонное, по видам сигнала, с программируемым пропуском, с выбором режима, по группам каналов памяти, с пропуском участка, программируемое, сканирование по пропускам, по каналам памяти, по каналам автосохранения, приоритетное сканирование. VSC, CTCSS, DTCS (тоновое) шумоподавление и шумоподавление по уровню входящего сигнала. VSC (голосовой шумоподавитель) открывается только когда поступает модулированный сигнал. Немодулированные сигналы или сигналы с интермодуляционным свистом (биением) игнорируются. Использование режима приема CTCSS и DTCS позволяет принимать сигналы только с соответствующим тоном. Помимо обычной системы шумоподавления, имеется система шумоподавления по уровню принимаемого сигнала, система приема сигнала с силой выше предустановленного уровня и система сигнализации о поступлении сигналов с подходящим тоном.

Совместимость с DSP-модулем. С дополнительным DSP-модулем UT-106 вы можете добавить больше функций цифрового шумоподавления, которые улучшают соотношение сигнал/шум. Также автоматический фильтр удаляет интермодуляционные свисты (биения). Функции DSP-модуля очищают полезный сигнал и обеспечивают превосходное качество приема.

**Другие функции DSP-модуля:**

- Выбор фильтра промежуточной частоты (ПЧ).
- Функция сдвига ПЧ (только SSB/CW-модуляция).

- Ограничитель импульсных помех (только SSB/CW/AM-модуляция) (подавляет импульсные помехи, например, от автомобильного зажигания).
- 20 дБ радиочастотный аттенюатор (ниже 1300 МГц).
- Автоматическая подстройка частоты (АПЧ).
- Автоматическая регулировка усиления (АРУ-переключение — Быстрое/Медленное).

**Другие функции:**

- Штормовое предупреждение (версия для США).
- Декодер DTMF.
- Дуплексная работа.
- Функция записи звука в формате WAV.
- Настраиваемые полосно-пропускные фильтры для VHF и UHF.

**Требования к компьютеру:**

Microsoft Windows XP/2000/ME/98SE, 50 Мб памяти на жестком диске, дисплей 1024×768, Intel Pentium III 450 МГц или выше, 128 Мб оперативной памяти или больше, порт USB 1.1.

**Комплектация:**

ПО, сетевой адаптер AD-113A/E (зависит от версии), антенна. USB-кабель.

| Технические характеристики | ICOM IC-PCR1500 | | | | |
|---|---|---|---|---|---|
| Диапазон частот, МГц | 0.01...3299,999 | | | | |
| Виды модуляции | SSB, AM, CW, FM, WFM | | | | |
| Чувствительность, мкВ (AM, SSB, CW при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | Диапазон, МГц | FM | WFM | AM | SSB, CW |
| | 0.495...1.799 | – | – | 25 | 5 |
| | 1.8...49.999 | 0.63 | – | 2.5 | 0.5 |
| | 50 – 699.999 | 0.5 | 1.4 | 2 | 0.4 |
| | 700 – 1300.000 | 0.63 | 1.8 | 2.5 | 0.5 |
| | 1300 – 2299.999 | 5.6 | 18 | – | – |
| | 2300 – 3000 | 18 | 0.25 | 1.0 | 0.4 |
| Количество каналов памяти | не ограничено | | | | |
| Потребляемый ток, мА | 0.8 (максимальная громкость) | | | | |
| Диапазон рабочих температур | –0°...+60 °C | | | | |
| Габариты и вес: основной блок | 146×41×206 мм, 1,2 кг | | | | |

## Icom IC-R1500 с компьютерным интерфейсом

Компания Icom представляет IC-R1500. Приемник охватывает диапазон частот от 0,01 до 3299,999 МГц с любым видом модуляции (в диапазоне от 0,495 до 1300 МГц работает только в режимах модуляции CW и SSB). Имеет функцию многоканального мониторинга, спектроскоп, поддерживает функцию сдвига промежуточной частоты (ПЧ), обеспечивает качественный и эффективный прием. Возможно подключение к компьютеру при помощи USB-интерфейса.

**Преимущества:**

Широкий диапазон: 0,01 – 3299,999 МГц с шагом от 1 Гц.

Два вида управления с компьютера либо при помощи управляющей панели.

Функция многоканального мониторинга.

Быстрое сканирование — до 60 каналов в секунду (зависит от возможностей компьютера).

VCS, CTCSS и DTCS тоновые шумоподавители.

Два вида спектроскопа.

Дополнительный DSP модуль, UT-106.

**Особенности:**

Широкополосный сканирующий приемник. Охватывает диапазон частот от 0,01 до 3299,999 МГц (зависит от версии) с любым видом модуляции (в диапазоне от 0,495 до 1300 МГц работает только в режимах модуляции CW и SSB). Шаг перестройки 1Гц. При подключении к компьютеру всеми его функциями легко управлять при помощи мыши и клавиатуры.

Виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM, включая специальные виды: узкая CW (2,8 кГц), широкая и узкая AM (2,8 / 6 / 15 / 50 кГц), широкая и узкая FM (6 / 15 / 50 / 230 кГц).

Пульт дистанционного управления IC-R1500 поставляется с панелью дистанционного управления. Подсветка дисплея трех цветов — желтого, зеленого и янтарного.

Быстрое сканирование — до 60 каналов в секунду. Скорость сканирования IC-R1500 до 60 каналов в секунду (ограничена возможностями компьютера) предоставляет высочайшую эффективность поиска в широком частотном диапазоне. Автоматическое запоминание каналов при поиске. В режиме сканирования с автоматической записью частот происходит запоминание частот найденных сигналов в специальный банк памяти.

Типы сканирования: диапазонное, по видам сигнала, с программируемым пропуском, с выбором режима, по группам каналов памяти, с пропуском участка, программируемое, сканирование по пропускам, по каналам памяти, по каналам автосохранения, приоритетное сканирование.

VSC, CTCSS, DTCS тоновое шумоподавление и шумоподавление по уровню входящего сигнала.

VSC (голосовой шумоподавитель) открывается только когда поступает модулированный сигнал. Смодулированные сигналы или сигналы с интермодуляционным свистом (биением) игнорируются. Использование режима приема CTCSS и DTCS позволяет принимать сигналы только с соответствующим тоном. Помимо обычной системы шумоподавления, имеется система шумоподавления по уровню принимаемого сигнала, система приема сигнала с силой выше предустановленного уровня и система сигнализации о поступлении сигналов с подходящим тоном.

Совместимость с DSP-модулем. С дополнительным DSP-модулем, UT-106 вы можете добавить больше функций цифрового шумоподавления, которые улучшают соотношение сигнал/шум. Также автоматический фильтр удаляет интермодуляционные свисты (биения). Функции DSP-модуля очищают полезный сигнал и обеспечивают превосходное качество приема.

Другие функции DSP-модуля:

- Выбор фильтра промежуточной частоты (ПЧ).
- Функция сдвига ПЧ (только SSB/CW модуляция).
- Ограничитель импульсных помех (только SSB/CW/AM модуляция) (подавляет импульсные помехи, например, от автомобильного зажигания).
- 20 дБ радиочастотный аттенюатор (ниже 1300 МГц).
- Автоматическая подстройка частоты (АПЧ).
- Автоматическая регулировка усиления (АРУ переключение — Быстрое/Медленное).
- Другие функции:
- Штормовое предупреждение (версия для США).
- Декодер DTMF.

- Дуплексная работа.
- Функция записи звука в формате WAV.
- Настраиваемые полосно-пропускные фильтры для VHF и UHF.
- 1000 каналов памяти.
- Все функции IC-R1500 доступны при подключении к компьютеру. Требования к компьютеру:

Microsoft Windows XP/2000/ME/98SE, 50 Мб памяти на жестком диске, дисплей 1024 × 768, Intel Pentium III 450 МГц или выше, 128 Мб оперативной памяти или больше, порт USB 1.1.

**Комплектация:**

ПО, сетевой адаптер AD-113A/E (зависит от версии), антенна, USB-кабель, панель управления, шнур панели управления (3,4 м).

| **Технические характеристики** | **ICOM IC-R1500** | | | | |
|---|---|---|---|---|---|
| Диапазон частот, МГц | 0.01...3299,999 | | | | |
| Виды модуляции | SSB, AM, CW, FM, WFM | | | | |
| Чувствительность, мкВ (AM, SSB, CW при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | Диапазон, МГц | FM | WFM | AM | SSB, CW |
| | 0.495...1.799 | — | — | 25 | 5 |
| | 1.8...49.999 | 0.63 | — | 2.5 | 0.5 |
| | 50 — 699.999 | 0.5 | 1.4 | 2 | 0.4 |
| | 700 — 1300.000 | 0.63 | 1.8 | 2.5 | 0.5 |
| | 1300 — 2299.999 | 5.6 | 18 | — | — |
| | 2300 — 3000 | 18 | 0.25 | 1.0 | 0.4 |
| Количество каналов памяти | не ограничено | | | | |
| Потребляемый ток, мА | 0.8 (максимальная громкость) | | | | |
| Диапазон рабочих температур (с панелью управления) | — 10... + 60 (— 0... + 60) °C | | | | |
| Габариты и вес: основной блок, панель управления | 146 × 41 × 206 мм, 1,2 кг (111 × 40 × 26,5 мм, 0,2 кг) | | | | |

## Icom IC-R10

Модель ICOM IC-R10 воплотила в себе все современные технологические достижения, что позволило добиться высококачественного приема сигналов всех видов модуляции в диапазоне от коротких волн до СВЧ при сохранении небольших габаритов и веса. Ряд функций (Voice Scan Control, Real-time Band Scope, SIGNAVI) впервые реализован в носимом сканере.

Расширенный набор типов и видов сканирования: каждый из двух основных типов сканирования (программируемое и по каналам

памяти) разбит на три вида: сплошное, диапазонное, с автоматической записью частот, по каналам памяти, по видам модуляции, по банкам памяти.

Новая функция SIGNAVI позволяет в несколько раз увеличить реальную скорость сканирования. При сканировании в режиме FM используется дополнительный приемный контур, который продолжает сканирование при нахождении основным приемником сигнала, таким образом, основной приемник сканирует скачками только по занятым каналам. Величина скачков составляет до 5 шагов настройки, но не более 100 кГц.

Компьютерный интерфейс. ICOM IC-R10 может быть подключен к компьютеру для клонирования или управления. Обмен данными осуществляется в разработанном ICOM формате CI–V через дополнительный блок CT-17 и позволяет как считывать данные (частоты, уровень сигнала), так и управлять всеми функциями приемника. Приемник ICOM IC-R10 поддерживается большинством управляющих программ (ARCON, SEDIF и др.). Для клонирования или программирования памяти требуется программа CS-R10 и кабель OPC-478.

| **Технические характеристики** | **ICOM IC-R10** | | | |
|---|---|---|---|---|
| Диапазон частот, МГц | 0.5...1300 | | | |
| Виды модуляции | SSB, AM, CW, FM, WFM | | | |
| Чувствительность, мкВ (AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | FM | 0.5...5МГц-0.5<br>5...200МГц- 0.32 | 200...340МГц-0.45<br>340...700МГц- 0.35 | 700...800МГц-0.79<br>800...1300МГц-0.5 |
| | WFM | 75...200МГц-1.0<br>200...240МГц-2.2 | 340...700МГц-1.3<br>700...800МГц- 2.0 | 800...900МГц-1.6 |
| | AM | 0.5...5 МГц-1.6<br>5...200 МГц- 1.0 | 200...340 МГц-1.6<br>340...700 МГц-1.4 | 700...800 МГц-2.0<br>800...1300 МГц-1.6 |
| | SSB, CW | 0.5...5 МГц-0.4<br>5...200 МГц- 0.25 | 200...340 МГц-0.4<br>340...700 МГц-0.32 | 700...800МГц-0.63<br>800...1300МГц-0.4 |
| Количество каналов памяти | 1000 | | | |
| Потребляемый ток max/min, мА | 180 / 38 | | | |
| Диапазон рабочих температур | –10...+50 °C | | | |
| Габариты и вес | 59×130×32 мм, 310 г | | | |

Расширенные функции использования памяти. 1000 каналов памяти разбиты на 18 банков (16 банков по 50 каналов, 2 банка по 100 каналов для автоматической записи частот и каналов пропуска). В каждом канале запоминается частота, вид модуляции (включая ширину полосы), шаг настройки и т. д. Каналам и банкам памяти можно присвоить буквенные имена длиной до 8 символов. Специальная EEPROM-память сохраняет информацию даже при севших аккумуляторах. Функция редактирования памяти позволяет производить копирование и вставку содержимого каналов.

Интеллектуальная система поиска голоса. VSC (Voice Scan Control) позволяет пропускать немодулированные и шумовые сигналы.

## Icom IC-R2

IC-R2 — представитель нового поколения сканирующих приемников. Главная его особенность — большие возможности в миниатюрном корпусе. Широкий диапазон: 0.495 — 1309.995 (разбит на 9 поддиапазонов) с шагом от 5 до 100 кГц. Виды модуляции: AM, FM, WFM, встроенный декодер тонов CTCSS. Функции прослушивания приоритетного канала (priority watch) и дуплексных каналов (offset monitor).

Простота в работе. Приемник имеет всего девять кнопок управления. Понятные символы на дисплее позволяют за несколько минут разобраться со всеми функциями.

Компактные размеры. Небольшой плоский корпус удобно ложится в вашу ладонь. Брызгозащищенное исполнение.

Гибкие возможности сканирования: по всему диапазону, в запрограммированных границах, по каналам памяти.

| **Технические характеристики** | **ICOM IC-R2** | | |
|---|---|---|---|
| Диапазон частот, МГц | 0.495...1309.995 | | |
| Виды модуляции | AM, FM, WFM | | |
| | FM | WFM | AM |
| Чувствительность, мкВ (AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | 1.6...5МГц-0.4<br>5...30МГц-0.25<br>30...118МГц-0.2<br>18...175МГц-0.18<br>175...470МГц-0.22<br>470...1000МГц-0.28<br>1000...1310МГц-0.45 | 30...118МГц-0.71<br>175...470МГц-0.71<br>470...1000МГц-1.0 | 0.5...5МГц-1.3<br>5...30МГц-0.79<br>118...136МГц-0.63<br>222...247МГц-0.63<br>247...330МГц- 0.71 |

| | |
|---|---|
| Скорость сканирования | до 30 каналов/сек |
| Количество каналов памяти | 450 (400 стандартных, 50 границ сканирования) |
| Потребляемый ток max/min, мА | 170 / 41 |
| Диапазон рабочих температур | −10...+60 °С |
| Габариты и вес | 58×86×27 мм, 170 г |

### Icom IC-R3

Носимый сканирующий приемник с возможностью просмотра видеоизображений.

Никогда ранее портативный приемник не предоставлял так много информации, как сейчас это может сделать ICOM IC-R3. Телевизионное изображение, спектр и многое другое можно увидеть на 2-дюймовом цветном TFT-экране.

Большой 2-дюймовый TFT-дисплей, позволяющий просматривать видеоизображения (PAL B/G, NTSC). Прием как телепрограмм и звука/разнос 4,5 или 5,5 МГц, так и видеоизображений со следящей камеры.

Расширенные функции использования памяти. 450 каналов памяти для удобства использования разбиты на 8 банков по 50 каналов. Один банк из 50 каналов используется для записи границ сканирования.

Автоматический шумоподавитель. Имеется возможность ручного управления шумоподавителем (9 уровней и полное открытие).

Li-ion аккумулятор и зарядное устройство входит в комплект поставки.

| **Основные технические характеристики** | **ICOM IC-R3** |
|---|---|
| Диапазон частот, МГц | 0,495...2450,095 |
| Виды модуляции | FM, AM, WFM, AM-TV, FM-TV |
| Шаг перестройки частоты, кГц | 5, 6.25 |
| Количество каналов | 450 (50×8 банков + 50×1 банк для записи границ сканирования) |

| Диапазон рабочих температур | — 10 ... + 60 °С | | | |
|---|---|---|---|---|
| Чувствительность, мкВ (при включенном предусилителе; SSB, CW, RTTY, AM — 10 дБ S/N; FM, WFM — 12 дБ SINAD) | FM | 0,5...5МГц-0,5<br>5...200МГц-0,32 | 200...340МГц-0,45<br>340...700МГц-0,35 | 700...800МГц-0,79<br>800...1300МГц-0,5 |
| | WFM | 75...200МГц-1,0<br>200...240МГц-2,2 | 340...700МГц-1,3<br>700...800МГц-2,0 | 800...900МГц-1,6 |
| | AM | 0,5...5МГц-1,6<br>5...200МГц-1,0 | 200...340МГц-1,6<br>340...700МГц-1,4 | 700...800МГц-2,0<br>800...1300МГц-1,6 |
| | SSB, CW | 0,5...5МГц-0,4<br>5...200МГц-0,25 | 200...340МГц-0,4<br>340...700МГц-0,32 | 700...800МГц-0,63<br>800...1300МГц-0,4 |
| Напряжение пит. /Ток потр. | 3,6...6,3 В /0,21 А (ном. громк., LCD — выкл.), 0,73 А (LCD — вкл.) | | | |
| Габариты и вес | 61 × 120 × 33 мм, 0,3 кг | | | |

## Icom IC-R5

IC-R5 — представитель нового поколения сканирующих приемников, дальнейшее развитие популярной модели IC-R2. Главные его особенности — большие возможности в миниатюрном корпусе при невысокой цене.

Широкий диапазон: 0.15 — 1309.995 МГц (разбит на 9 поддиапазонов) с шагом от 5 до 100 кГц.

Виды модуляции: AM, FM, WFM, встроенный декодер тонов CTCSS и DTCS.

Функции прослушивания приоритетного канала (priority watch) и дуплексных каналов (offset monitor).

Простота в работе. Приемник имеет всего девять кнопок управления, понятные символы на дисплее позволяют за несколько минут разобраться со всеми функциями. Компактные размеры. Плоский корпус небольших размеров удобно ложится в вашу ладонь. Брызгозащищенное исполнение. Гибкие возможности сканирования: по всему диапазону, в запрограммированных границах, по каналам памяти.

Автоматический шумоподавитель.

Знакосимвольный дисплей с подсветкой.

До 100 мВт акустической выходной мощности.

Приемник работает от двух элементов питания типа АА.

Разъем для подключения наушника и внешнего источника питания.

Функции клонирования и программирования памяти с компьютера.

| Технические характеристики | ICOM IC-R5 | | |
|---|---|---|---|
| Диапазон частот, МГц | 0.495...1309.995 | | |
| Виды модуляции | AM, FM, WFM | | |
| Чувствительность, мкВ (AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | FM | WFM | AM |
| | 1.6...5МГц-0.4<br>5...30МГц-0.25<br>30...118МГц-0.2<br>118...175МГц-0.18<br>175...470МГц-0.22<br>470...1000МГц-0.28<br>1000...1310МГц-0.45 | 30...118МГц-0.71<br>175...470МГц-0.71<br>470...1000МГц-1.0 | 0.5...5МГц-1.3<br>5...30МГц-0.79<br>118...136МГц-0.63<br>222...247МГц-0.63<br>247...330МГц-0.71 |
| Скорость сканирования | до 30 каналов/сек | | |
| Количество каналов памяти | 450 (400 стандартных, 50 границ сканирования) | | |
| Потребляемый ток max/min, мА | 170 / 41 | | |
| Диапазон рабочих температур | −10°...+60 °C | | |
| Габариты и вес | 58×86×27 мм, 170 г | | |

## Icom IC-R20

IC-R20 является малогабаритным профессиональным широкодиапазонным сканирующим РПУ с возможностью регистрации принимаемого сигнала на встроенный цифровой магнитофон и одновременного контроля двух частот.

***Двойной прием:*** До появления ICOM IC-R20 для слежения за двумя частотами было необходимо использовать два приемника. Теперь стало возможным слежение за аварийными каналами, контроль над воздушным движением, наблюдение за двумя водителями, прием одновременно радио и ТВ-сигнала.

***Широкий диапазон — от КВ до СВЧ:*** ICOM IC R20 работает на частотах от 150 кГц до 3304,999 МГц в режимах SSB, CW, AM, FM, WFM с шагом перестройки от 0,01 до 100 кГц. Это позволяет принимать AM/FM-радиодиапазоны, телевизионные сигналы, радиосвязь между кораблями, самолетами, выполнять другие технические задачи.

***Цифровой диктофон на 4 часа:*** 32-мегабайтный цифровой магнитофон сканера ICOM R20 непрерывно осуществляет в течение четырех часов запись принимаемого сигнала, сохраняет принятые с эфира радиопередачи и позволяет их перезаписывать через USB-порт в ПЭВМ.

Благодаря функции записи сигнала на встроенный магнитофон возможно производить запись трансляции с беспроводного (радио) микрофона в ходе переговоров. Через USB-порт можно переписать в компьютер принятую передачу или переслать по назначению. (Прослушивание на компьютере невозможно.)

***Прием сигналов с кодовым и тональным разделением каналов.*** Когда многочисленные пользователи находятся на одном канале, они используют специальную систему разделения каналов для уменьшения помех от других пользователей. Две наиболее популярные системы реализованы в ICOM R 20, это DTCS и CTCSS. По субтонам возможно сканирование.

***Большая память с буквенными наименованиями каналов.*** 1000 стандартных каналов памяти, 200 автоматически сканируемых каналов и 25 пар границ сканирования. IC-R20 позволяет удобно настраиваться и записывать в память частоты сигнала с возможностью присвоения каждому каналу отдельного имени.

***До 11 часов непрерывной работы.*** Экономичность, присущая аппаратуре фирмы ICOM, реализована и в IC-R20: 11 часов работы без подзарядки от встроенного Li-Ion аккумулятора. Также ICOM R-20 может работать от трех пальчиковых батареек AA. Длительная работа, так же как и зарядка встроенного аккумулятора, возможна от прикуривателя автомобиля или входящего в комплект адаптера.

***Функции сканирования.*** IC-R20 — самый быстрый сканирующий приемник фирмы ICOM. Скорость сканирования — до 100 каналов в секунду в режиме VFO. Вы можете поместить каналы памяти внутрь динамически изменяемых банков (до 100 каналов в банке, не более 26 банков), кроме того, можно связать несколько различных банков для сканирования по банкам памяти. Дополнительно ICOM IC R20 предлагает разнообразный контроль за сканированием, например, задержка сканирования, возобновление сканирования при определенном сигнале и т. д.

***Функция спектроанализа (Real-time bandscope):*** Спектроскоп работает в реальном времени и позволяет контролировать наличие сигналов. Иногда прослушивания сигнала недостаточно, поэтому IC R20 имеет спектроскоп. Он используется для отображения сигнала, на частоту которого настроен приемник. Спектроскоп работает независимо от прослушивания сигнала. Дополнительная функция спектроскопа заключается в возможности определения модулированности сигналов.

| Технические характеристики ICOM 1C R20 | |
|---|---|
| Одновременный прием двух полудуплексных частот:<br>VFO A<br>VFO B | 0.150 – 469.999МГц (LSB, USB, CW, AM, FM, WFM)<br>118 – 174.999, 330 – 1304.999MHz (AM, FM, WFM) |
| виды модуляции | LSB*, USB*, CW*, AM, FM, WFM (* 0.150469.999МГц) |
| количество каналов | 1250 (1000 основных, 50 сканируемых границ и 200 автоматически записываемых) |
| шаг перестройки частоты, кГц | 0.01, 0.1, 5, 6.25, 8.33*, 9*, 10, 12.5, 15, 20, 25,30, 50, 100КГц |
| питание | 4 BP-206 или 3 батареи типа AA (R6) 8В (4 AA (R6) Ni-Cd аккумулятора) 4,8 – 16В (источник постоянного тока) |
| ток потребления, мА | прием: 150 (подсветка выключена) режим готовности: 100 (подсветка выключена) режим энергосбережения: 35 |
| тип разъема под антенну | BNC (500м) |
| вес, г | 320 |
| размеры, мм | 60 × 142 × 34,8 |
| диапазон рабочих температур, °С | от – 10 до + 60 |
| чувствительность (SSB, CW, AM — 10 дБ S/N; FM, WFM — 12 дБ SINAD)<br>FM<br>FM<br>AM<br>SSB, SW | 1.620 – 4.999МГц — 0.56 мкВ<br>5.000 – 221.999МГц — 0.4 мкВ<br>330.000 – 832.999МГц — 0.56 мкВ<br>833.000 – 1304.999МГц — 0.71 мкВ<br>1330.000 – 2304.999МГц — 5.6 мкВ<br>2330.000 – 2999.999МГц — 18 мкВ<br>76.000 – 108.000МГц — 1.8 мкВ<br>175.000 – 221.999МГц — 1.8 мкВ<br>470.000 – 769.999МГц — 2.5 мкВ<br>0.495 – 4.999МГц — 2.2 мкВ<br>5.000 – 29.999МГц — 1.4 мкВ<br>118.000 – 135.999МГц — 1.4 мкВ<br>0.495 – 4.999МГц — 0.4 мкВ<br>5.000 – 29.999МГц — 0.25 мкВ<br>50.000 – 53.999МГц — 0.25 мкВ<br>118.000 – 146.999МГц — 0.25 мкВ<br>330.000 – 469.999МГц — 0.32 мкВ |
| избирательность, дБ | SSB, CW: более 1.8кГц/-6дБ<br>FM, AM: более 12кГц/-6дБ, менее 30кГц/-60дБ<br>WFM: более 150кГц/-6дБ |

## Icom IC-R8500

Новейшие технологические достижения позволили фирме ICOM добиться высококачественного приема сигналов всех видов модуляции в диапазоне от коротких волн до СВЧ при постоянной чувствительности. ICOM IC-R8500 — это не просто сканер, это профессиональный связной приемник с широким набором специальных функций — начиная от скоростного сканирования и кончая развитым компьютерным интерфейсом.

Широкий диапазон: 0,1 — 2000 МГц с шагом 10 Гц.

Виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM, включая специальные виды: узкая CW, широкая и узкая AM, узкая FM (для приема узкой CW требуется фильтр FL-52A).

Сверхвысокая стабильность частоты. Высокостабильный кварц (TCXO) обеспечивает стабильность менее +/-100Гц (до 30 МГц) и менее 0,3 ppt (свыше 30 МГц), что повышает качество работы схем PLL и DDS.

Повышенное качество приема. Схемы сдвига промежуточной частоты (IF shift) и режекторный аудиофильтр (APF) впервые встроены в приемник такого класса. Сдвиг ПЧ позволяет разделить близкорасположенные сигналы. Режекторный фильтр используется для подавления интерференции от наложенных друг на друга сигналов, что особенно эффективно при работе с CW. Качество приема повышается также за счет применения шумоподавителя (NB), ВЧ-аттенюатора, переключаемой АРУ и цифровой АПЧ. Чувствительность приемника в диапазоне от 2 до 1300 МГц практически не зависит от частоты.

Расширенные функции использования памяти. В каждом канале запоминается частота, вид модуляции (включая ширину полосы), шаг настройки и т. д. Для повышения эффективности память разделена на 20 банков по 40 каналов и на области автоматической записи или пропуска по 100 каналов. Каналам и банкам памяти можно присвоить буквенные имена длиной 8 и 5 символов соответственно. Дополнительно в памяти выделено 20 каналов для границ сканирования и 4 приоритетных канала. Количество каналов в каждом банке может быть изменено. Функция редактирования памяти позволяет производить копирование и вставку содержимого каналов.

Компьютерный интерфейс. На задней панели приемника расположен не только разъем CI—V, но и последовательный порт для не-

посредственного подключения к компьютеру. Обмен осуществляется в разработанном фирмой ICOM формате CI—V и позволяет как считывать данные (частоты, уровень сигнала), так и управлять всеми функциями приемника. Приемник ICOM IC-R8500 поддерживается большинством управляющих программ (ARCON, FILIN и др.).

7 типов сканирования: программируемое, диапазонное, по каналам памяти, по видам сигнала, по группам каналов памяти, приоритетное, с автоматической записью частот. Скорость сканирования плавно регулируется до 40 каналов в секунду (как в режиме сканирования по каналам памяти, так и при программируемом сканировании). Время задержки также плавно регулируется. Интеллектуальная система поиска голоса. VSC (Voice Scan Control) позволяет пропускать модулированные и шумовые сигналы.

Удобство настройки. Предусмотрено два метода ввода частоты: с клавиатуры или с помощью ручки настройки. Шаг настройки регулируется в пределах от 10 Гц до 1 МГц. Дополнительно существует режим программируемого шага, устанавливаемого для каждого канала в пределах от 0,5 до 100 кГц с разрешением 0,5 кГц.

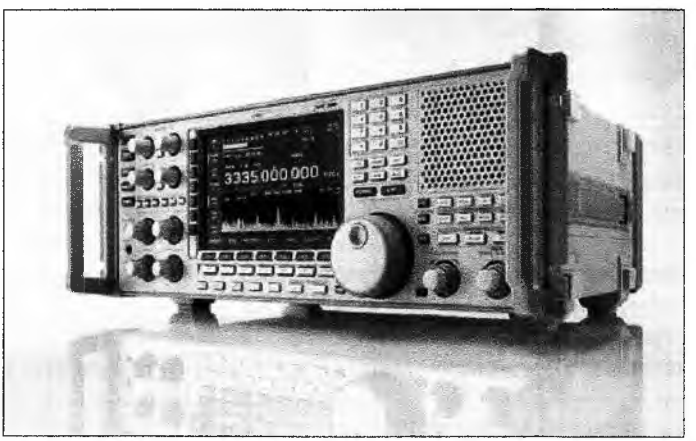
**Прочие функции:**

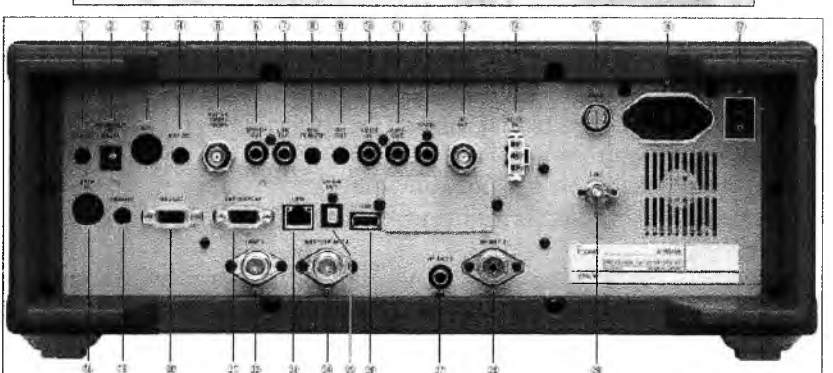
Автоматическое выключение (Sleep timer). 3 антенных разъема — SO-239, RCA и N-type. Стрелочный S-метр и индикатор центральной частоты. Шумоподавитель с предустановкой порогового уровня сигнала. Разъемы REC и REC-remote для записи сигналов и управления магнитофоном.

| **Технические характеристики** | **ICOM IC-R8500** | | | | | | |
|---|---|---|---|---|---|---|---|
| Диапазон частот, МГц | 0.1...2000 | | | | | | |
| Виды модуляции | SSB (USB, LSB), AM (wide, normal, narrow), CW (normal, narrow), FM | | | | | | |
| Чувствительность, мкВ (SSB, CW, AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | Диапазон, МГц | SSB, CW | AM | AM-N | AM-W | FM | WFM |
| | 0.1...0.5 | 1.0 | 6.3 | — | — | — | — |
| | 0.5...1.8 | 2.0 | 13.0 | — | — | — | — |
| | 1.8...2.0 | 0.25 | 3.2 | 3.5 | — | — | — |
| | 2.0...28 | 0.2 | 2.5 | 2.0 | — | — | — |
| | 28...30 | 0.2 | 2.5 | 2.0 | — | 0.6 | — |
| | 30...1000 | 0.32 | 3.6 | 2.0 | 3.2 | 0.5 | 1.4 |
| | 1240...1300 | 0.32 | 3.6 | 2.0 | 3.2 | 0.5 | 2.0 |
| Количество каналов памяти | 1000 стандартных, 20 границ сканирования, 1 приоритетный | | | | | | |

| | |
|---|---|
| Потребляемый ток, А | 2.0 |
| Диапазон рабочих температур | −10... + 50 °С |
| Скорость сканирования | 10 − 40 каналов в секунду (при сканировании из памяти и программируемом канале) |
| Габариты и вес | 287 × 112 × 309 мм, 7,0 кг |

## Icom IC-R9500

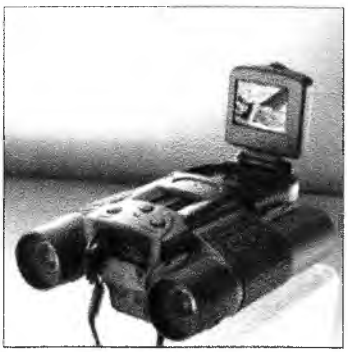


1. External Speaker Jack
2. External DC Output Jack (13.8V)
3. ACC Socket
4. Antenna Selector Jack
5. Reference Frequency In/Out Terminal
6. Speech Output Jack
7. Line Output Jack
8. Recorder Remote Jack
9. Detector Output Jack
10. Video Input Jack
11. Video Output Jack
12. Spare Jack
13. IF Output Jack
14. DC DC Power Socket
15. Fuse Holder
16. AC Power Socket
17. Main Power Switch
18. Data Input Socket
19. CI-V Remote Control Jack
20. RS-232C Connector
21. External Display Connector
22. Antenna Connector 2
23. Ethernet Connector
24. Antenna Connector 1/ HF Antenna Connector 3
25. S/P DF Output Terminal
26. USB Connector
27. HF Antenna Connector 2
28. HF Antenna Connector 1
29. Ground Terminal

## 3.12. Оптические приборы

### Бинокль-видеокамера




Данный бинокль обладает множеством полезных функций: это и цифровая камера, и веб-камера, и полноценный бинокль.

**Тактико-технические характеристики:**
Оптический сенсор — CMOS 300KPX.
Внутренняя память — 8Mb SDRAM.
Режимы камеры — видеозапись (без звука), фотоснимки, web-камера.
Разрешение — 640×480(VGA)/352×288(CIF).
Хранение данных — в формате JPEG VGA — 75, CIF — 300.
Внешний дисплей — LCD, монохромный.
Подключение к ПК — USB 1,1.
Выдержка — 1/4 – 1/1000 сек.
Фокусное расстояние линз — 28 мм.
Фокусировка — 2 см — бесконечность.
Питание — от USB, автономно — 2 AAA батарейки (в комплект не входят).
Прочее — таймер автоотключения, таймер снимка, индикатор батарей, сигнал малого заряда.
Габариты — 96 мм × 119 мм × 49 мм.
Вес — 300 г (без батарей).

### Зрительная труба Kowa TD-1

Telephoto Spotting Scope/Digital Camera. Помимо простого наблюдения, данный прибор позволяет проводить качественную видеосъемку и фотографирование на дистанции до 1,5 км, оставаясь незаметным для объекта наблюдения.

**Тактико-технические характеристики:**

Встроенная 3,2-мегапиксельная цифровая камера.
Разрешение 2048 × 1536, 1024 × 768.
Запись на SD Memory Card.
Дисплей размером 1,8 дюйма (4,6 см).
Инфракрасный пульт в комплекте.

**Характеристики:**

Код товара: TD-1.
Корпус: серебристый.
Кратность увеличения: 10×-30×.
Диаметр объектива: 55.
Рабочее расстояние от окуляра до глаза (мм): 20.

# Глава 4. Организация защиты информации

Комплекс мер по защите объекта от утечки информации включает в себя подготовительные и основные мероприятия, причем как технического, так и организационного и правового характера.

## 4.1. Подготовительные мероприятия

### 4.1.1. Организационные мероприятия (ОМ)

Процесс организации защиты информации проходит поэтапно.

**Первый этап**

состоит в том, чтобы определить, что нужно защищать. Анализ проводится по следующим направлениям:

- какая информация нуждается в защите;
- наиболее важные (критические) элементы защищаемой информации;
- определяется срок жизни критической информации, т. е. время, необходимое конкуренту для реализации добытой информации;
- определяются ключевые элементы (индикаторы) информации, отражающие характер охраняемых сведений;
- индикаторы классифицируются по функциональным зонам предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения, управления и т. д.).

**Второй этап**

(выявление угроз):

- определяется, кого может заинтересовать защищаемая информация;
- оцениваются методы, используемые конкурентами для получения этой информации;
- оцениваются вероятные каналы утечки информации;
- разрабатывается система мероприятий по пресечению действий конкурентов.

**Третий этап**
подразумевает анализ эффективности принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т. д.).

**Четвертый этап**
определение необходимых дополнительных мер защиты на основе проведенных исследований на первых трех этапах, например, ужесточение пропускного режима, установка автоматизированных систем управления и контроля доступом, введение конфиденциально делопроизводства, замена действующих пропусков новыми, закупка поисковой техники и т. д.

**Пятый этап**
руководством предприятия (фирмы) рассматриваются представленные предложения по всем необходимым мерам безопасности и рассчитывается их стоимость и эффективность.

**Шестой этап**
реализация принятых дополнительных мер безопасности с учетом установленных приоритетов.

**Седьмой этап**
осуществление контроля исполнения принятых мер и доведения до персонала фирмы реализуемых мер безопасности.

### 4.1.2. Технические мероприятия (ТМ)

Технические мероприятия по защите информации обычно проводятся параллельно с организационными и начинаются со второго этапа организационных мероприятий.

**Технические мероприятия включают в себя:**
- изучение объекта;
- оперативно-технический осмотр территории и помещений объекта;
- инженерно-техническое оборудование объекта;
- профилактические осмотры;
- постоянные, временные и эпизодические мероприятия по защите каналов утечки информации при помощи технических средств.

Одним из основных направлений специальной (технической) защиты является проведение оперативно-технического осмотра.

***Оперативно-технический осмотр (ОТО)*** — комплексная проверка территории и помещений объекта с целью оценки безопасности объекта и обнаружения подслушивающих устройств.

На основе данных, полученных в ходе осмотра, разрабатывается и выполняется комплекс мероприятий, исключающих возможность утечки и перехвата информации в дальнейшем.

Оперативно-технический осмотр также включает в себя несколько этапов:

**1. Изучение объекта.**

Цель изучения объекта перед проведением ОТО — определение вероятного противника, оценка его оперативных и технических возможностей по проникновению на объект с целью съема информации.

Техника съема информации не может появиться на объекте сама по себе, ее должен кто-то принести в интересующее противника помещение и правильно там установить. Для этих целей используют, как правило, таких сотрудников объекта (или лиц, периодически его посещающих), как монтер-телефонист, электрик, уборщица или мебельщик. Люди этих специальностей периодически работают в кабинетах, где ведутся разговоры, где хранится и обрабатывается разнообразная информация. В периоды нахождения в помещениях этой категории лиц имеется достаточно времени для тщательного изучения и подбора мест установки техники съема информации, проведения проверки эффективности работы спецсредств, замены элементов электропитания и демонтажа спецтехники после окончания срока ее работы.

На рабочем столе перед проведением важного совещания, переговоров или беседы можно подменить какой-либо предмет на точно такой же, но с электронной «начинкой», а затем вернуть все на свое место. Следует учитывать ситуации, когда спецтехника может быть спрятана в подарки или сувениры, которыми часто украшают кабинеты и комнаты для переговоров. Наиболее удобной ситуацией для внедрения разнообразной техники подслушивания является капитальный или косметический ремонт кабинета и всего объекта.

Классическим местом для техники подслушивания является телефон. В современных электронных телефонных аппаратах весьма сложно обнаружить скрыто установленную спецтехнику. Нередко электронные элементы аппарата могут сами являться подслушивающими устройствами даже без их предварительной переделки. В связи с этим рекомендуется устанавливать в кабинетах, где проводятся

важные совещания и переговоры, только те телефоны, которые рекомендованы специалистами и предварительно ими проверены. Проводя изучение объекта и помещения, следует также оценивать уровень противника, спецтехнику которого предполагается обнаружить. В самом деле, невозможно подходить с одними и теми же методами защиты от ЦРУ или коммерческой структуры; помимо большого различия в финансовых и технических возможностях, у них совершенно разные интересы в объекте.

В зависимости от вероятного противника, тактика проведения поисковых мероприятий может существенно различаться — от демонстративной открытой поисковой работы до целого комплекса конспиративных мероприятий. Определив противника, можно оценить технические и оперативные возможности, которые он мог бы использовать на объекте. Так, чтобы капитально установить спецтехнику в ограждающие конструкции (стены, пол и потолок), надо располагать достаточно большой (3—5 человек) технически подготовленной бригадой и возможностью конспиративного захода на объект и в помещение хотя бы на несколько часов.

В то же время радиозакладку может в течение нескольких минут внедрить и неспециалист во время одного кратковременного захода в помещение (кабинет).

Следует также учитывать, что радиозакладки со сложными системами кодирования и передачи информации коммерсанту, например, ни за какие деньги приобрести невозможно, так как они изготавливаются только по заказу спецслужб и строго учитываются. Далее при изучении объекта поиска следует уделить самое пристальное внимание расположению помещения и режиму посещения как его, так и смежных с ним кабинетов. Так, например, если оно граничит с ванной комнатой, то у противника имеется реальная возможность, не привлекая внимания, засверлить с этой стороны акустический канал и установить спецаппаратуру.

Наличие стенных шкафов с коммуникациями в смежном коридоре также дает хорошие возможности для внедрения спецтехники. Особенно сложной является ситуация, когда в помещении не контролируется смена предметов мебели и интерьера, прокладка коммуникаций и прочие действия, что создает реальные предпосылки для внедрения подслушивающих устройств. В таких случаях весьма сложно провести локализацию канала утечки информации, определить, кто и когда установил подслушивающее устройство и, соответственно, какая информация попала к противнику.

Если оперативным путем получены данные о наличии канала утечки, то анализ информации позволит определить примерное вре-

мя внедрения, а сопоставление его с другими событиями (ремонт, смена мебели и т. д.) — и место установки техники. Также следует обращать внимание на поведение телефонных линий — непонятные «безадресные» звонки, «подзвонка», искажения в линии и т. д. Можно попытаться «проиграть» мероприятие по внедрению спецтехники, т. е. посмотреть на объект глазами противника. Для этого надо «подобрать» места расположения пунктов приема информации, проработать режим их обслуживания (контроль за аппаратурой, смена кассет, обеспечение безопасности). Затем с этих позиций изучить еще раз окружение объекта.

Таким образом, оперативное изучение объекта позволяет оценить наиболее вероятные пути поиска и наиболее подозрительные места, выработать тактику проведения поисковых мероприятий. Целесообразно составить план-схему помещений, схему коммуникаций и определить материал ограждающих конструкций. На основании этого определяется тип аппаратуры и тактика ее использования. Естественно, если существуют материалы предыдущих поисковых мероприятий, они должны быть тщательно изучены и постоянно использоваться при поиске для сравнения результатов.

**Указанная выше работа по изучению объекта сводится к следующим мероприятиям:**

1) определение вероятного противника и оценка его оперативно-технических возможностей по проникновению в помещение;
2) изучение расположения помещения и его окружения;
3) изучение режима посещения, порядка установки в нем предметов интерьера, мебели, проведения ремонтных работ;
4) установка всех фактов ремонта, монтажа или демонтажа коммуникаций, замены мебели или предметов интерьера;
5) изучение конструктивных особенностей здания и ограждающих конструкций помещения;
6) изучение всех коммуникаций, входящих в помещение или проходящих через него.

**После завершения изучения объекта необходимо провести работы по подготовке к проведению поисковых мероприятий.**

**2. Составление плана ОТО.**

Для этого необходимо выработать методику поиска на конкретном объекте и составить перечень поисковой аппаратуры.

Вначале ***определяются группы и способы проверки*** (см. таблицу).

| № | Группа проверки | Способы проверки |
|---|---|---|
| 1. | Предметы, содержащие электронику | — разборка;<br>— визуальный осмотр;<br>— сравнение с эталонами;<br>— рентгенографирование (просмотр с помощью рентгеновских снимков). |
| 2. | Мебель и предметы интерьера | — осмотр металлоискателем;<br>— осмотр нелинейным локатором;<br>— рентгенографирование (просмотр с помощью рентгеновских снимков). |
| 3. | Электроустановочные изделия | — осмотр нелинейным локатором;<br>— рентгенографирование (просмотр с помощью рентгеновских снимков). |
| 4. | Коммуникации | — осмотр детектором коммуникаций;<br>— осмотр трассоискателем;<br>— проверка тестером. |
| 5. | Ограждающие конструкции | — осмотр металлоискателем;<br>— осмотр нелинейным локатором. |

Такая последовательность является оптимальной. Она может меняться в зависимости от различных обстоятельств, например, при наличии отдельного помещения, в которое предварительно можно вынести все предметы интерьера, в первую очередь те, которые могут оказаться источниками помех и ложных срабатываний на последующих этапах.

После определения групп и способов обследования ***определяются сроки и последовательность поисковых мероприятий***, которые зависят от объема работ по каждому способу, количества аппаратуры и опыта поисковиков.

Особое внимание следует уделить электромагнитной совместимости аппаратуры, например, работая с нелинейным локатором, можно «обнаружить» другие поисковые аппараты.

Особое внимание при подготовке плана поиска следует уделить отмеченным на этапе изучения ***подозрительным и наиболее уязвимым местам*** объекта и помещения. В этих местах целесообразно проведение исследований несколькими способами, например, нелинейная локация в сочетании с рентгеноскопией (просмотр с помощью рентгеновского аппарата).

Для каждого из направлений поиска следует ***предварительно выработать модель технического средства вероятного противника***. Так, если планируется искать проводные коммуникации, проложенные профессионалами из спецслужб, то рентгеновский аппарат должен давать разрешение менее 1 мм, а если же противник — коммерческая структура, то достаточно 2—3 мм. Проволочки соответствующего диаметра должны быть включены в тест, кото-

рый будет подкладываться при каждой съемке для определения точности обследования.

Аналогично готовятся тесты и для других исследований. Зачастую вполне достаточно использовать образцы спецтехники, которые, по вашему мнению, соответствуют уровню противника. Так, для поиска изделий, внедренных противником, возможности которого не превышают возможности коммерческих структур, вполне достаточно приобрести на рынке несколько образцов радиомикрофонов отечественного и зарубежного производства. Подготовив модели и используя их перед каждой проверкой, можно быть уверенным, что ваш поисковый аппарат позволяет в данном конкретном месте обнаружить любые устройства, не превосходящие по классу вашу модель.

Отдельным пунктом плана поискового мероприятия является ***контроль эфира в месте проведения поиска***. Здесь особое внимание следует уделить конспиративности работ, чтобы внешнему наблюдателю было невозможно привязать работу оператора радиоконтроля к поисковой бригаде. Контроль эфира должен начинаться за несколько дней до прибытия бригады и завершаться через несколько дней после окончания работ. На этапе подготовки также должны быть спланированы ***действия бригады в случае обнаружения канала утечки информации или скрыто установленной спецтехники***. Это может быть, как демонстративный поиск, когда работы не скрываются и изъятие производится сразу же после обнаружения, так и конспиративный поиск, когда обнаруженный канал используется для передачи дезинформации или «закрывается» искусственно создаваемыми помехами, которым должен быть придан характер естественных (установлен кондиционер, вентилятор и т. п.).

Конспиративный поиск по многим причинам является более предпочтительным:

***во-первых,*** появляется возможность локализовать утечку информации, определить возможного установщика и контролера спецтехники, начать подготовку «закрытия» канала дезинформацией или помехами;

***во-вторых,*** можно на основании анализа технических характеристик канала попытаться провести оперативный поиск в местах наиболее вероятного расположения пункта приема информации и выйти на «заказчика»;

***в-третьих,*** повышается безопасность поисковиков, поскольку возможны попытки препятствования их работе (в зарубежных условиях это провокация и высылка из страны, а в условиях России — прямое физическое воздействие).

В связи с этим ***в плане поискового мероприятия должны быть:***

- четко разработанная легенда появления поисковиков в обследуемом объекте и вообще в городе;
- линия поведения поисковиков при проведении работ: молчание или разговоры на темы, не связанные с поиском, маскировка шумов аппаратуры бытовыми шумами и т. д.;
- действия по закрытию канала утечки каким-либо источником шума до полного окончания работ. Необходимо, чтобы этот источник естественно вписывался в линию поведения владельца помещения или легенду присутствия бригады. Так, если работы ведутся под легендой ремонта, то наличие в бригаде «меломанов», с утра до вечера слушающих поп-музыку, не вызовет подозрений. Необычной будет ситуация, когда владелец кабинета «ни с того ни с сего» стал слушать подобное круглые сутки.

Легендирование поисковых мероприятий и работ по подготовке к ним должно быть уделено самое тщательное внимание, так как от этого в большой степени зависит безопасность и результативность мероприятия, достоверность его результатов. Например, для неподготовленного в оперативном плане сотрудника объекта или его окружения может показаться странным приезд, например, в Красноярск из Москвы бригады для проведения косметического ремонта кабинета одного из руководителей. Гораздо более убедительной может быть другая причина — монтаж и наладка аппаратуры спецсвязи.

При подготовке оперативного обеспечения поиска следует также учитывать необходимость удаления из обследуемых помещений всех лиц, в том числе и знающих о характере и задачах работ. Чем меньше людей знакомы с техникой и методикой проведения работ, тем более они успешны, тем меньше возможность утечки информации к противнику.

Руководитель бригады проводит изучение объекта и разрабатывает план поискового мероприятия, особенно оперативной его части.

**Руководитель бригады должен:**

- установить контакт с лицом, ответственным за безопасность объекта;
- разработать с ним легенду своего появления при изучении объекта;
- получить от него или через него ответы на все вопросы, необходимые для изучения объекта и подготовки мероприятия;
- разработать и согласовать план оперативного обеспечения мероприятия;

- решить вопросы доставки и хранения поисковой аппаратуры на объекте, порядка ее заноса в обследуемое помещение, размещение членов бригады и их доступ в здание в соответствии с выработанной легендой.

**Итоговыми документами при подготовке мероприятия являются:**

- План оперативных мероприятий по прикрытию работы поисковиков;
- План оперативных мероприятий по локализации канала утечки при его обнаружении;
- Перечень лиц, посвященных в характер работ;
- План проведения радиоконтроля с подобранными и проверенными местами установки радиоаппаратуры;
- План прилегающей местности в радиусе до 1000 м с указанием по возможности принадлежности зданий, особенно находящихся в прямой видимости окон помещения (желательно с фотографиями или видеосъемкой);
- Поэтажные планы здания с указанием всех помещений, смежных с обследуемым, характеристики стен, перекрытий, материалов отделки и коммуникаций, а также сведения о лицах, занимающих смежные помещения, и о режиме их посещения;
- План-схема коммуникаций всего объекта с указанием всех щитов и разводных коробок;
- План обследуемого помещения с указанием всех предметов интерьера мебели и оборудования, электроустановочных изделий и средств связи;
- План проведения работ с указанием сроков, последовательности и исполнителей;
- Перечень особо подозрительных мест и отдельный план их обследования;
- Модель ожидаемой на объекте спецтехники для проверки эффективности поиска;
- Легенда проведения поисковых работ;
- План действий на случай обнаружения спецтехники или канала утечки информации;
- Перечень поисковой аппаратуры.

**3. Подготовка сил и средств для проведения ОТО.**

На этом этапе производится:

- подбор и расстановка сотрудников по участкам работы;
- инструктаж сотрудников по действиям в ходе проведения ОТО;

— проверка работоспособности поисковой аппаратуры и других средств;
— определение времени начала и окончания работ.

**4. Оперативно-технический осмотр объекта.**

В ходе проведения поискового мероприятия выполняются следующие работы:

**1. Контроль радиоэфира**

Поисковое мероприятие начинается с изучения оперативной обстановки вокруг объекта:

- определения вероятного расположения контрольных пунктов (КП) приема информации от спецтехники, возможно установленной на объекте;
- оперативная разработка предполагаемых КП;
- фиксирование подозрительных автомашин, стоящих подолгу с пассажирами и без них, появляющихся и исчезающих вместе с владельцем проверяемого помещения;
- ведение конспиративного наблюдения за ними.

Далее организуется работа пункта контроля радиоэфира (ПКР).

Вначале ПКР должен быть развернут в здании объекта или рядом с ним, но не в проверяемом помещении. Основные цели работы ПКР:

- составление карты занятости эфира в районе проведения мероприятия;
- выделение и исключение из дальнейшего анализа сигналов легальных (известных) радиостанций;
- статистический анализ работы подозрительных станций.

Такой радиоконтроль может продолжаться несколько дней, затем ПКР переносится в проверяемые помещения и принимаемые в нем сигналы сравниваются с полученной ранее статистикой.

Особое внимание уделяется сигналам, уровень которых при переносе ПКР в проверяемые помещения возрос. Эти сигналы берутся на особый контроль, осуществляется их разработка, изучение содержания информации с целью нахождения источника сигнала.

Если сигнал при перемещении внутри помещения или по помещениям меняется резко, то источник сигнала находится в ближней зоне, внутри здания или на территории и для его локализации можно дополнительно использовать индикаторы поля, желательно со встроенным частотомером или применять отдельно переносной частотомер. В этом случае возможно определение параметров разрабатываемого сигнала.

Также следует уделить внимание сигналам, которые «синхронизированы» с появлением или уходом владельца помещения или сотрудников бригады поисковиков.

Контроль эфира должен продолжаться в течение всего мероприятия и еще несколько дней после его окончания. Вполне возможно, что противник расшифровал работу бригады и выключил на это время устройства съема информации, а после окончания поиска он будет пытаться включить их снова.

Во время поискового мероприятия необходимо несколько раз переносить ПКР в пределах помещения и здания, постоянно сравнивая получаемые результаты. Это повышает вероятность обнаружения источника сигнала на объекте.

**2. Визуальный осмотр**

Поиск в конкретном помещении начинается с его визуального осмотра. Вначале проводится сравнение с планами, идентификация предметов мебели и интерьера. По возможности все устройства, содержащие электронику, должны быть вынесены из помещения и обследованы отдельно.

Во время визуального осмотра основное внимание уделяется бросовым (быстро заносимым) предметам, происхождение которых точно неизвестно.

Также тщательно осматриваются все полости и щели в плинтусах, полах и за батареями отопления, труднодоступные места на шкафах, карнизах и т. п. Вся мебель отодвигается, вынимаются и осматриваются ящики, внутренние полости.

Вскрываются и осматриваются электророзетки и выключатели, разбирается электроустановочная арматура, просматриваются стояки и вводы коммуникаций в помещении и около него. По возможности все провода и коммуникации прослеживаются визуально и с помощью эндоскопов. При этом необходимо строго придерживаться правил безопасности работы с электросетью — отключать электрощиты, пользоваться индикаторами сети, резиновыми перчатками и защитными ковриками.

**3. Проверка электронных приборов**

Проверка устройств с электронными компонентами является наиболее сложным делом, так как здесь практически неприменимы аппаратурные методы. Основа работы в этом случае — сравнение с эталоном. Электронные устройства вскрывают и осматривают с целью выявления изменений схемы и появления дополнительных конструкций, сделанных не на заводе.

Следует особое внимание уделять подпайкам к проводам питания. Дело в том, что полностью внедрить устройство съема инфор-

мации в промышленное изделие можно только в заводских условиях, поэтому более быстрым, относительно простым и потому наиболее вероятным способом внедрения является подсоединение устройства съема к цепи питания с помощью проводников.

Конечно, определить назначение всех элементов, например, в компьютере, очень сложное дело. Эта работа под силу только специалистам, однако, при внимательном просмотре можно определить следы элементов, установленных вне заводского цикла: следы паек, изменение цвета покрытия в местах подпаек и прочие отметки вмешательства.

Большим подспорьем является наличие эталона, т. е. аналогичного образца, в «чистоте» которого есть уверенность. Поэтому необходимо заранее узнать марки всех электронных изделий и подобрать их эталоны. С них удобнее всего сделать фотографии и рентгенограммы для последующего сравнения с проверяемым образцом. Особое внимание следует обращать на элементы усилений корпуса электронных приборов. В их утолщениях можно легко разместить радиомикрофон.

В дальнейшем фотографии и рентгенограммы обследованных электронных приборов можно использовать при повторной проверке, уже в качестве эталона.

Отдельно рентгенографируются конденсаторы, особенно в телефонных аппаратах, поскольку радиомикрофоны часто «заделываются» именно в конденсаторы. Перед разборкой электронных приборов, например, современных телефонных аппаратов, они проверяются с помощью индикатора поля и частотомера на наличие излучений как во включенном (телефонные аппараты со снятой трубкой), так и в выключенном состоянии (соответственно с положенной трубкой). При наличии подозрительных излучений, которые регистрируются индикатором на расстоянии 60 — 80 см от прибора, необходимо настроить комплекс радиоконтроля на эту частоту и, облучая проверяемый прибор акустическим сигналом, искать признаки модуляции в принимаемом радиосигнале.

В качестве облучаемого сигнала лучше всего использовать генератор с резко меняющимся уровнем (типа сирены), а наблюдать принимаемый сигнал на анализаторе спектра или осциллографе, подключенном к приемнику ПКР.

Указанный способ проверки радиосигналов дает положительный эффект даже в том случае, когда в радиомикрофоне используется необычный вид модуляции или шифрация. В этом случае акустический сигнал модуляции как бы «перегружает» передатчик и в его радиосигнале это можно выявить.

Если «под рукой» нет анализатора спектра, можно воспользоваться и наушниками, но оценка становится более субъективной. В этой ситуации целесообразно повторить исследование обнаруженного радиосигнала без проверяемого устройства — его необходимо убрать в соседнее помещение. Такую проверку целесообразно проводить и при наличии анализирующих приборов. Если обследование проводится в большом помещении, то возможна ситуация, когда, облучая акустическим сигналом один проверяемый прибор, обнаруживается канал утечки от другого устройства.

Изделие с обнаруженным таким образом каналом утечки информации необходимо затем тщательно проверить всеми возможными средствами. Как показывает практика, необязательно в нем обнаружится внедренная спецтехника. Чаще всего канал утечки информации создается в электронных устройствах за счет конструктивных особенностей и даже дефектов. Зафиксированы случаи, когда повышенный уровень излучения гетеродина в сочетании с плохим креплением его тонкостенного экрана превращал радиоприемник в передающее устройство с радиусом действия до сотни метров, да к тому же с хорошей акустической разборчивостью. Такие блоки электронных устройств, как звонок электромеханического телефона или шаговый двигатель электрических часов могут являться микрофонами, и, подключившись с помощью довольно несложной аппаратуры к проводке, можно контролировать помещение, не заходя в него, с расстояния в несколько десятков метров.

Проверяемые электронные устройства, у которых обнаружены паразитные (т. е. возникающие за счет дефектов конструкции) каналы утечки информации, должны быть удалены из помещения. Необходимо также предупреждать владельца кабинета или делать официальное письмо-заключение о выключении приборов с обнаруженными паразитными излучениями при ведении служебных и конфиденциальных разговоров. При возможности следует заменять или удалять электронные приборы с паразитными излучениями из рабочих кабинетов.

**4. Проверка предметов интерьера и мебели**

Проверка мебели, куда относятся все подвижные предметы (книги, карнизы, статуэтки, папки с бумагами, пепельницы), начинается с их тщательного визуального осмотра.

Особое внимание следует уделить всякого рода укрепляющим броскам-подставкам и способам их крепления, поскольку аппаратура подслушивания, закамуфлированная под элементы мебели, крепится, как правило, на шипах или тому подобных элементах, позво-

ляющих при необходимости установить спецтехнику в течение нескольких секунд.

Одновременно визуально проверяются ультрафиолетовые (или другие невидимые) метки, поставленные в предыдущие обследования на мебель и предметы интерьера.

Затем готовится площадка для проведения аппаратурной проверки, при которой обычно используются нелинейный локатор, металлоискатель и рентгеновский аппарат.

Сначала площадка проверяется выбранным типом поисковой аппаратуры (локатором или металлоискателем) на наличие помеховых сигналов. Определяются источники помех и, по возможности, устраняются, например, переносятся, или идентифицируются по направлению так, чтобы при обследовании была возможность развернуть поисковый аппарат в противоположном направлении.

Если, например, помеховый сигнал идет от стены, то при развороте антенны нелинейного локатора, т. е. при обследовании предмета в направлении «от стены», помеха значительно ослабнет. Убедиться в том, что сигнал ложный, можно и путем перемещения обследуемого предмета при неподвижном поисковом приборе. При этом если уровень сигнала от поискового прибора практически не меняется, то сигнал ложный.

Затем, убедившись в том, что сигнал идет именно от обследуемого предмета, следует внимательно осмотреть место, откуда идет сигнал, и произвести рентгенографирование его. Если сигнал возникает за счет крепежных элементов (гвозди, болты и т. д.), то следует попытаться запомнить особенности сигнала — при работе с нелинейным локатором это тембр сигнала, его уровень, характерные трески при простукивании места отклика. При работе с металлоискателем — это только местоположение и размеры.

Желательно проверять предметы несколькими типами поисковых приборов. Аппаратное обследование предметов мебели и интерьера следует проводить при минимально возможном потенциале (минимальной чувствительности) поисковых приборов, предварительно проверив работоспособность с помощью модели (теста). Предмет проверяется с различных направлений, чтобы точнее зафиксировать направление на источник сигнала.

В зависимости от материала обследуемого предмета выбирается поисковый прибор. Для деревянных изделий лучше использовать металлоискатель, например, малогабаритный вихревой металлоискатель.

При обследовании металлоискателем необходимо проводить им по предмету в разных направлениях и с разным расположением ан-

тенны. Практика работы с металлоискателем позволяет получать довольно большую точность, до нескольких миллиметров.

При сравнении обследуемого предмета с другими, аналогичными по назначению и конструкции, можно определить аномальные места. Нелинейный локатор в таких случаях менее точен, однако он незаменим при работе с предметами, содержащими большое число металлоконструкций.

Дешифровка сигналов нелинейного локатора производится на слух, например, путем довольно энергичного простукивания узлов соединений, поскольку в этих местах практически всегда существует нелинейность, образующаяся за счет контактов разнородных металлов или окисных пленок. Качество таких полупроводниковых свойств низкое, поэтому нелинейный локатор будет давать «хриплый» тон, который при простукивании модулируется или может вообще исчезнуть.

Все сомнения относительно источника отклика может рассеять рентгенография. Лучше всего сделать рентгенограммы типовых узлов креплений, а затем использовать их при рентгеноскопии для сравнения. Следует, однако, помнить, что рентгенография достаточно трудоемкий процесс, который требует наличия фотолаборатории, что не всегда возможно.

Более мобильной и, следовательно, легко применимой в обычных условиях является рентгеноскопия. Если при этом используются специальные «запоминающие» экраны, то при значительном ухудшении разрешающей способности рентгеноскопия вполне может заменить рентгенографию.

После окончания проверки на всю мебель и предметы интерьера наносятся незаметные, например, видимые только в ультрафиолетовых лучах, метки, которые потребуются при последующих проверках. Составляется опись предметов, находящихся в помещении, которая хранится вместе с уточненным планом помещения у лица, ответственного за его безопасность, или в учреждении, проводящем поисково-защитные мероприятия.

**5. Проверка электроустановочных и коммуникационных изделий**

При проведении этого этапа работ следует соблюдать правила электробезопасности и обесточить помещение до начала работ. После этого прослеживаются все трассы сильно- и слаботочной проводки, определяются разводные коробки. Затем снимаются все розетки, выключатели, осветительные приборы и прочие электроустановочные изделия и все рентгеноскопируются.

Необходимо внимательно осматривать подводящие провода в местах установки коммуникационных изделий; максимально их вытягивать из закладных труб, так как места выхода провода из труб

являются наиболее удобными для подключения и установки радиомикрофонов с электропитанием от сети.

Аппаратурное обследование электрокоммуникаций проводится со стороны вводного электрощита. Необходимо точно установить электролинии, идущие в обследуемое помещение; убедиться в том, не подключены ли к ним другие помещения, иначе вы «обнаружите» телевизор или радиоприемник в соседнем кабинете. Если по общей схеме электропитания здания обследуемое помещение не отделено от остальных автоматом защиты или по соображениям конспирации невозможно находиться у щита с поисковой аппаратурой, тогда помещение отсоединяется от общей сети на входной вводной коробке, а поисковый аппарат подключается к ней с помощью временной линии.

Затем необходимо прикинуть длину проводки внутри помещения и на максимальном удалении от прибора подключить штатный имитатор или выбранную модель вероятной спецтехники.

После этого в соответствии с инструкцией на детектор коммуникаций проводятся исследования линии в режиме холостого хода, а затем в режиме короткого замыкания (поочередно закорачивая все ветви цепи).

Следует отметить, что аппаратурное обследование можно проводить и не снимая электроустановочные изделия, однако если обнаружится отклик — их все равно придется снимать, так что лучше это сделать сразу.

При поиске коммуникаций необходимо использовать трассоискатель, реагирующий на магнитное поле силовой проводки. Для идентификации электролиний со стороны разводных коробок и к нему подсоединяется тестер. Затем поочередно, закорачивая провода в местах установки коммуникационных изделий, по сопротивлению определяется принадлежность линии. Наиболее удобным является тестер со звуковой сигнализацией короткого замыкания.

Затем линия размыкается и измеряется сопротивление изоляции, которое должно быть в пределах единиц Мом. Если величина сопротивления отличается, то данную ветвь следует внимательно обследовать — «пройти» вдоль нее нелинейным локатором для поиска подозрительных мест, «запитывая» линию от детектора коммуникаций. Если подозрительных сигналов нет, то желательно все же заменить данную линию в соответствии с нормами на электропроводку.

Возможна проверка линий на наличие в них передач как в речевом, так и в надтональном спектре. Для этого используются усилители или приемники, подключаемые к линии, а также специальные сканирующие устройства. При этом линия должна прослушиваться в нагруженном режиме.

Указанные выше обследования целесообразно проводить до проверок с отключением линии.

Обследование слаботочных коммуникаций (трансляционная сеть, охранная и пожарная сигнализации, телевидение, селекторная связь и др.) проводится по методике, аналогичной вышеприведенной, с учетом их схемных особенностей.

Обследование телефонных линий имеет свои особенности, поскольку если вышеперечисленные коммуникации могут использоваться противником только для передачи информации или в качестве источников питания, то телефонная линия используется еще и как источник информации. В соответствии с этим она должна подвергаться дополнительным обследованиям.

Телефонные коммуникации должны обследоваться по максимально возможной длине (идеально — до кросса АТС) теми же методами, что и другие коммуникации. На практике проводят проверку линии до вводной коробки в здание, со стороны которой подключается поисковый прибор. В этом случае можно делать вывод об отсутствии подключений только до той точки, где подключался поисковый прибор. Серьезный противник может подключиться к магистральному телефонному кабелю на улице или на АТС.

Телефонные линии обследуются под нагрузкой индикатором поля или другим устройством контроля эфира. Для этого имитируется разговор по телефонной линии, а поисковик перемещается вдоль проводки с индикатором поля или другим средством контроля эфира. В случае обнаружения подозрительных излучений имитируется многократное рассоединение. Если в этом случае уровень подозрительного сигнала меняется синхронно с рассоединением, то обнаруженный сигнал необходимо поставить на контроль ПКР для дальнейшей дешифровки. При необходимости ПКР можно перемещать вдоль телефонной линии для определения расположения источника излучения.

Этот метод позволяет выявлять подключения подслушивающих устройств с передачей по радиоканалу, находящихся также и вне проверяемого участка, поскольку будет иметь место «наводка» сигнала на телефонную линию. После окончания проверки все установочные изделия маркируются, составляется полная схема сильно- и слаботочных коммуникаций.

Весьма желательно затем опечатать все коммуникационные коробки, щиты и телефонные аппараты лицом, ответственным за безопасность объекта.

**6. Проверка ограждающих конструкций**

Эта работа является заключительным этапом аппаратурных обследований. Основным поисковым инструментом здесь является не-

линейный детектор, особенно в случае бетонных ограждающих конструкций.

Перед началом обследований нелинейным локатором осматриваются все смежные с проверяемым кабинетом помещения, в том числе и на прилегающих этажах, убираются как можно дальше от смежных стен или по возможности выносятся устройства, содержащие электронику: видео- и аудиотехника, оргтехника, факсимильные аппараты, электронные телефонные аппараты и т. д.

Затем проводится моделирование на каждой из обследуемых поверхностей, для чего модель крепится с одной стороны стены, а аппарат устанавливается с другой так, чтобы приемопередающая антенна вплотную прилегала к поверхности, и определяются минимальные регулировочные уровни нелинейного локатора, при котором модель обнаруживается.

После работы с моделью обследуется поверхность стены в соответствии с методикой использования нелинейного локатора (у разных моделей могут быть разные скорости перемещения, различные способы анализа и т. д.). При обнаружении отклика фиксируется его местоположение с помощью клейкой ленты или другим способом. При первом «проходе» стены нелинейным локатором, особенно на относительно небольших поверхностях, рекомендуется сначала пройти всю площадь стены и зафиксировать отклики, а уже затем приступать к их дешифровке. Это связано с тем, что большинство откликов возникает от таких элементов, как арматура, сетка-рабица, гвозди, проводка, трубы и т. п.

Обследуя первоначально всю поверхность стены, можно заметить характерные отклики, прикинуть причины их возникновения, оценить количество ложных откликов.

Для дешифрации откликов используется снижение чувствительности и мощности облучения нелинейного локатора — чем ниже эти потенциалы, тем точнее антенна указывает на место источника.

Затем по характеру отклика определяется его природа, например, классический полупроводник дает «чистый» сильный тон. При работе нелинейным локатором мощностью облучения порядка 300 Ватт можно попытаться «выжечь» коррозионный полупроводник или же разрушить его сильным простукиванием поверхности стены резиновым молотком.

Ложный полупроводник имеет «исчезающий» отклик; при простукивании у него появляется модуляция и возможны резкие изменения уровня сигнала отклика.

Места, в которых отклик вызывает сомнения, лучше всего вскрыть и найти причину срабатывания нелинейного локатора. Для

более полной расшифровки откликов иногда используют и другой прием — нелинейный локатор переносится на противоположную сторону стены и снова контролируется подозрительный отклик. Часто это приводит к исчезновению отклика, что свидетельствует о ложном (коррозионном) полупроводнике.

При обследовании деревянных стен и конструкций следует помнить о большой проникающей способности нелинейного локатора. На практике иногда возникали ситуации, когда локатор фиксировал телевизор «насквозь» через несколько помещений.

Своеобразные эффекты могут наблюдаться при обследовании металлических оконных рам, если рядом работает мощная телевизионная или радиостанция. Наличие разнородных металлических элементов превращает ее в «диполь с установленными между плечами диодами». Такая конструкция сильно переизлучает попадающие на нее сигналы и может имитировать подслушивающее устройство. Избавиться от такого эффекта (или снизить его) можно, открывая рамы на 90 градусов и сильно их простукивая.

Также сильно осложняется обследование помещений вблизи проходящих в стенах электрических и водяных коммуникаций, около стояков телевизионных антенн. Сигнал передатчика нелинейного локатора «наводится» на металлические трубы коммуникаций и, отражаясь затем от других металлоконструкций, дает ложные срабатывания нелинейного локатора. В высотных зданиях, например, часто прослушивается характерная работа водяных насосов, которые периодически подкачивают воду.

Поэтому рекомендуется отдельно обследовать нелинейным детектором стояки коммуникаций: если сигнал периодически повторяется вдоль стояка, то, вероятнее всего, это наводка.

Обнаруженные нелинейным локатором подозрительные места целесообразно рентгенографировать. При этом следует только помнить, что каждые 10 КВ напряжения на трубке излучателя рентгеновского аппарата позволяют просветить примерно 1 см толщины стены или предмета. Таким образом, для просвечивания стен толщиной 10 см требуется аппарат с трубкой на 100 КВ.

При анализе подозрительных мест, обнаруженных поисковыми приборами, следует учитывать выбранную на этапе подготовки модель вероятного противника, т. е. имеется ли у него возможность установить технику съема информации в стену или нет. Практика показывает, что внедрение спецтехники в ограждающие конструкции требует большой подготовки и существенных материальных затрат, а также благоприятных условий для работы на объекте (капитальный ремонт, строительство и т. п.). Менее сложным является

путь внедрения спецтехники с внешней стороны стены, иногда для этих целей используют естественные ниши в ограждающих конструкциях.

При обследовании ограждающих конструкций необходимо учитывать и возможность установки противником так называемых «безнакольных» микрофонов или электронных стетоскопов. Наиболее возможный путь внедрения такой спецтехники — это приклеивание с внешней стороны интересующих противника помещений. Балки, трубы, цельнолитые бетонные стены и другие несущие строительные конструкции здания могут хорошо проводить звуковые сигналы на десятки метров, поэтому электронные стетоскопы могут быть установлены достаточно далеко от обследуемого помещения. В процессе поиска стетоскопов следует обращать внимание на указанные элементы конструкций, проходящие около или через обследуемое помещение, и с помощью измерительного электронного стетоскопа измерить направление и дальность распространения по ним акустических сигналов.

Определенная таким образом зона возможной установки стетоскопов обследуется затем визуально и с помощью поисковой аппаратуры. В реальных условиях стетоскоп противника, установленный достаточно далеко от объекта его заинтересованности, будет собирать шумы от всех мест, через которые проходит элемент конструкции, на котором стетоскоп установлен. В этом случае разборчивость информации будет весьма невысока, но тем не менее о наличии таких каналов утечки информации надо знать и рекомендовать зашумление их естественными шумами, например, поставить рядом холодильник или, еще лучше, кондиционер.

**5. Подготовка отчетных документов по итогам ОТО.**

После обследования объекта готовятся отчетные документы. Форма отчетности может быть произвольной. Желательным является описание и схемы мест срабатывания поисковой аппаратуры, вскрытий стен, мебели, предметов интерьера и технических устройств.

Важным моментом отчета о поисковом мероприятии является вывод с обоснованием о степени защищенности объекта от несанкционированного съема информации. Дополнением к отчету о поиске могут быть рекомендации (предписания) о мерах (работах, мероприятиях) по усилению специальной защиты объекта, его конкретных помещений.

Поисковые мероприятия должны регулярно проводиться сотрудниками службы безопасности, при этом их проведение требует наличия у исполнителя определенных навыков и квалификации.

## 4.2. Основные мероприятия

Для обеспечения комплексной защиты информации организуется:
— правовая защита;
— организационная защита;
— инженерно-техническая защита.

Правовая защита обычно реализуется централизованно, в масштабах всего предприятия (компании) или отдельных организаций, а организационная и инженерно-техническая защита — как централизованно, так и децентрализованно — по объектам, с учетом конкретных особенностей защищаемых информационных ресурсов и мест их размещения.

### 4.2.1. Правовая защита

заключается в обеспечении возможности применения к нарушителям информационной безопасности адекватных мер с использованием норм всех видов права с целью возмещения причиненного ущерба или локализации его последствий.

Для всеобъемлющей правовой защиты интересов предприятия (фирмы) используются:

1) законы, другие акты и документы правового, нормативного и рекомендательного характера, перечисленные в главе 1;
2) нормы авторского права, патентования и лицензирования;
3) правовые основы, заложенные в устав предприятия (фирмы), и документы, регулирующие трудовые отношения.

Правовая защита информации на предприятии (в фирме) предполагает юридическое закрепление:

1) взаимоотношений предприятия (фирмы) и государства по поводу правомерности использования системы защиты информации на данном предприятии (в фирме);
2) взаимоотношений фирмы и персонала по поводу обязанности персонала соблюдать установленные меры защитного характера;
3) ответственности персонала за нарушение порядка защиты информации.

Последний элемент включает:

- наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, трудовых договорах, в должностных инструкциях положений и обязательств по защите конфиденциальной информации;
- формулирование и доведение до сведения всех сотрудников положения о правовой ответственности за разглашение конфиден-

циальной информации, несанкционированное уничтожение или фальсификацию документов;
- разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.
- В числе основных подсистем защиты информации в правовом плане можно считать:
- установление на объекте режима конфиденциальности;
- разграничение доступа к информации;
- правовое обеспечение процесса защиты информации;
- четкое выделение конфиденциальной информации как основного объекта защиты.

Опираясь на государственные правовые акты на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности.

К таким документам относятся:
- Политика информационной безопасности;
- Положение о коммерческой тайне;
- Положение о защите персональных данных;
- Перечень сведений, составляющих конфиденциальную информацию;
- Инструкция о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;
- Положение о специальном делопроизводстве и документообороте;
- Обязательство сотрудника о сохранении конфиденциальной информации;
- Памятка сотруднику о сохранении коммерческой тайны.

Указанные нормативные акты направлены на предупреждение случаев неправомерного оглашения (разглашения) секретов на правовой основе, и в случае их нарушения должны приниматься соответствующие меры воздействия. Как правило, к работнику применяются меры дисциплинарного воздействия, например, штраф или лишение премии. Применение же более строгих мер, таких как привлечение к административной и уголовной ответственности, практически не используется ввиду причин, рассмотренных нами в главе 1.

### 4.2.2. Организационная защита

заключается в регламентации технологических процессов и деятельности сотрудников на нормативно-правовой основе таким обра-

зом, что реализация угроз информационной безопасности становится невозможной или существенно снижается. Организационная защита является ключевым направлением в обеспечении безопасности, объединяющим меры правовой и инженерно-технической защиты в единый комплекс, а также позволяет нейтрализовать угрозы, против которых правовая и инженерно- техническая защита неэффективна.

Подразделениями безопасности с целью установления режимов безопасности в деятельности предприятия (фирмы) в сфере своей компетенции разрабатываются и вводятся в действие установленным порядком необходимые нормативные и методические документы, подлежащие обязательному исполнению.

К организационной защите относятся мероприятия, обеспечивающие:

1. Подбор, расстановку и обучение сотрудников, обеспечение их персональной ответственности за соблюдение режимов безопасности.
2. Установление порядка допуска* к информации.
3. Разработку и установление режима и правил использования информации.
4. Установление и поддержание пропускного и внутриобъектового режимов.
5. Высокую личную безопасность сотрудников.
6. Выбор эффективных способов и экономное распределение сил и средств, используемых для защиты информации.
7. Защиту информации в случаях и при обстоятельствах, когда правовая и инженерно-техническая защита недостаточно эффективна или нецелесообразна.
8. Учет требований безопасности при проектировании, строительстве и оборудовании зданий и помещений, выбор имеющихся зданий и помещений под размещение структурных подразделений и для обработки и хранения информации.
9. Создание резервных копий наиболее ценных информационных ресурсов, организация их надежного хранения.
10. Разработку кризисных планов на случай реализации угроз безопасности или возникновения непредвиденных ситуаций, а также мер по локализации и компенсации нанесенного ущерба.
11. Обеспечение вновь создаваемых структурных подразделений необходимыми техническими системами и средствами безопас-

---

* Допуск — право (процедура предоставления права) лиц и организаций на проведение каких-либо работ или на доступ к чему-либо (куда-либо).

ности, нормативными, организационными и методическими документами по информационной безопасности.

К основным организационным вопросам, таким образом, можно отнести:

- Организацию охраны, пропускного и внутриобъектового режима. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц.
- Организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая их обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации.
- Организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.
- Организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации.
- Организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты.
- Организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

### 4.2.3. Инженерно-техническая защита

Инженерно-техническая защита заключается в использовании:

1) специфических свойств зданий и помещений, основных и вспомогательных технических систем и средств, транспортных средств;
2) различных специализированных технических систем и средств безопасности с целью исключения или максимально возможного ослабления вероятности нанесения ущерба в случае реализации угроз безопасности.

Меры инженерно-технической защиты применяются в целях:

1) обеспечения жизни и здоровья сотрудников — носителей информации;

2) создания условий для надежной сохранности информации при ее хранении, использовании и перевозке;
3) исключения проникновения на территорию объектов, в здания и помещения посторонних лиц*;
4) защиты информации в информационной (компьютерной) системе предприятия (фирмы) от несанкционированного доступа;
5) защиты информации от утечки по техническим каналам;
6) резервирования наиболее важных основных и вспомогательных технических средств и систем защиты информации, их энергоснабжения;
7) осуществления независимого и объективного контроля за сотрудниками и событиями, накопления регистрационной информации.

Разработка инженерно-технической защиты предприятия — головная боль службы безопасности и руководства ЧОПа, а не рядовых охранников, что, в свою очередь, не мешает грамотному охраннику или телохранителю вносить указанным лицам предложения по закупке того или иного оборудования для улучшения действующей системы защиты. А что касается мероприятий, непосредственно касающихся указанных сотрудников, например, оперативно-технического осмотра автомобиля или кабинета охраняемого лица, то тут они просто обязаны это делать.

Другой вопрос, что делать это надо обдуманно. А то другой раз приходит горе-телохранитель к руководству и просит купить для служебной надобности какой-нибудь прибор за пару сотен тысяч рублей. В итоге получает закономерный вопрос — зачем? И стоит родимый сопли жует: «Типа так на всякий случай. Вдруг когда-нибудь пригодится». И что ему скажет руководитель? Правильно. Пошлет подальше. Потому что четкого обоснования необходимости закупки нет. А вот выбросить на ветер двести тысяч ему совсем не хочется. Поэтому, прежде чем что-то просить, вы должны точно представлять: 1) какие служебные вопросы вам поможет решить данный прибор; 2) хватит ли у вас знаний и навыков для работы с ним; потребуется ли дополнительное обучение для работы с прибором, сколько оно будет стоить и сколько займет времени; 3) можно ли будет вам учиться с отрывом от работы и т. д. Для чего это нужно? А чтобы не купить дорогую игрушку, которую вы либо сразу сломаете, либо она будет валяться без дела, так как вы не сможете с ней работать. Во всех случаях ответственность за случившееся ля-

* Посторонние лица — все лица, в том числе и сотрудники фирмы, не имеющие разового, временного или постоянного допуска на объект или к защищаемому ресурсу.

жет на вас, как на инициатора закупки, причем и материальная тоже.

Кроме того, надо трезво оценивать рынок аппаратуры защиты информации. Большинство приборов опробованы только в лабораторных условиях и не соответствуют заявленным характеристикам. Чтобы взять действительно стоящую вещь, надо побегать по выставкам, проконсультироваться со специалистами, причем с теми, кто реально их применяет на практике, почитать отзывы пользователей в СМИ, наконец, протестировать прибор самим. Вот тогда вам станет понятно, нужен он вам или нет.

Короче говоря, объем работы очень немаленький. И, несмотря на вашу, возможно, скромную роль в системе безопасности организации, уважающий себя сотрудник должен как минимум представлять весь объем этой работы и разбираться в ряде ключевых моментов.

# Глава 5. Технические средства защиты информации

После того, как мы определились с тем, как организуется защита информации, пора познакомиться с техническими средствами, которые помогают нам обнаружить и локализовать каналы утечки информации. Указанная техника подразделяется на две основные группы: 1) поисковая техника; 2) техника защиты информации.

## 5.1. Поисковая техника

### 5.1.1. Досмотровые зеркала и эндоскопы

#### Досмотровое устройство «Перископ-165»

**Назначение**

Для визуального досмотра транспортных средств, грузов, труднодоступных и плохо освещенных мест в помещениях. Устройство незаменимо в работе правоохранительных органов, служб безопасности, а также может использоваться в быту.

**Особенности**

«Перископ-165» состоит из телескопической углепластиковой штанги и набора сменных зеркал различной площади и конфигурации. Длина штанги регулируется в пределах от 550 мм (транспортное положение) до 1650 мм. Вес устройства — 0,3 кг. Для подсветки осматриваемой поверхности используются два излучающих светодиода, встроенные прямо в штангу. Это уникальное решение используется в досмотровых устройствах впервые. В качестве источника питания используются три батарейки типа ААА. Заряда батареек хватает на 8 часов непрерывной работы светодиодов.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Облегченная телескопическая штанга (углепластик) — четырехсекционная | |
| max длина | 1650 мм |
| min длина | 550 мм (транспортировочное положение) |
| регулировка длины грубая | от 600 мм до 950 мм |
| регулировка длины плавная | от 950 мм до 1650 мм |
| Сменные зеркала | |
| Круглое, диаметр | 0 130 мм |
| Круглое, диаметр | 0 130 мм |
| Круглое, диаметр | 0 90 мм |
| Круглое, диаметр | 0 60 мм |
| Прямоугольное | 60 мм × 110 мм |
| Подсветка | |
| Источник света | два излучающих светодиода |
| Освещенность — на расстоянии 500 мм от наблюдаемого объекта | 1,6 Кд |
| Источник питания | батарейки типа ААА — 3 штуки |
| Время непрерывной работы светодиодов | не менее 8 часов |
| Масса изделия в сборе | 0,3 кг |

## Досмотровое зеркало «Поиск-СМТ»

**Назначение**

Досмотровые зеркала могут быть использованы ГИБДД, МЧС, ФСБ, ФСО, КПП любых ведомств и организаций при осмотре днищ и колес автомобилей, труднодоступных мест в строительных конструкциях, на кораблях, при обследовании развалин зданий, также удобны при поиске взрывчатых веществ и других устройств.

**Особенности**

Компактное складное зеркало для поисковых работ под транспортными средствами. СМТ можно носить в кармане как дополнение к ведению персональной защиты. Снабжено выпуклым зеркалом, телескопической рукояткой и миниатюрным фонарем. Зеркало может быть настроено под разнообразными углами и обеспечивает

широкий угол обзора. Уникальная телескопическая рукоятка очень прочная, для обеспечения недрожащего изображения.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| В рабочем положении длина рукоятки | 460 мм |
| Габаритные размеры зеркала в сложенном состоянии | 155 × 90 × 20 мм |
| Питание фонаря | от 2 батарей AAA |
| Масса | 260 г |

## Телевизионное досмотровое устройство Поиск-ТВ

**Назначение**

Предназначено для досмотра труднодоступных мест в помещениях, транспортных средствах, грузах и других объектах, а также применяется для поиска пострадавших людей в завалах зданий, дистанционного осмотра полостей завалов, определения состояния пострадавших путем их осмотра, а также обследования конструкции завала для выбора оптимальной технологии его разбора. Осмотр осуществляется с помощью установленной на конце штанги малогабаритной телевизионной камеры с ИК-подсветкой. Устройство позволяет осуществлять наружное наблюдение из-за преград и через оконные проемы.

**Особенности**

Телевизионное изображение наблюдаемых объектов представляется на экране ЖК-монитора, возможно дополнительное оснащение устройства встроенным модулем памяти и модулем трансляции ТВ-изображения на расстояние до 200 м. Применение ИК-подсветки позволяет обеспечить скрытность досмотра в условиях внешнего затемнения. Устройство выпускается в двух модификациях: с ручным или механическим дистанционным управлением положением модуля телекамеры. Устройство переносится в штатной упаковке — кофре.

**Базовый комплект поставки**

- Телескопическая штанга с модулем телекамеры.
- Блок питания и управления (БПУ).
- Аккумулятор.
- Зарядное устройство (ЗУ).
- Кабель соединительный.
- Жилет (для размещения и ношения БПУ).
- Штатная упаковка.
- Руководство по эксплуатации.
- Формуляр.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Угол обзора модуля телекамеры | не менее 72° × 54° |
| **Диапазоны регулировки с фиксацией промежуточных значений:** | |
| длина телескопической штанги | от 550 до 1550 мм |
| угол поворота стержня держателя камеры относительно оси штанги | от 0° до 210° |
| Разрешение модуля телекамеры со встроенной ИК-подсветкой в центре экрана | не менее 390 ТВЛ |
| **Электропитание прибора** | |
| от сети | 220±10%В, 50 Гц |
| от аккумулятора | напряжением 12 В, емкостью 3,8 А-часа |
| Потребляемая мощность | не более 15 Вт |
| Время непрерывной работы от блока питания и управления (БПУ) с полностью заряженным аккумулятором в нормальных климатических условиях | не менее 5,0 часов |
| Автоматическая индикация разряда аккумулятора при уменьшении напряжения на его клеммах до величины | 11 + 0,2 В |
| Поле обзора телекамеры, град | 120 |
| Разрешение в центре экрана, ТВЛ | 380 |
| Размер экрана ЖК-монитора по диагонали, мм | 102 |
| **Габаритные размеры** | |
| длина штанги в сложенном состоянии, мм | не более 550 |
| длина штанги при полностью раздвинутых звеньях, мм | не менее 1550 |
| БПУ | не более 180 × 260 × 60 мм |
| Габаритные размеры штатной упаковки, мм | 650 × 310 × 110 |

| Масса не более | |
|---|---|
| штанги | 0,6 кг |
| БПУ (с аккумулятором) | 1,5 кг |
| прибора в штатной упаковке | 5,7 кг |
| Время развертывания прибора в рабочее состояние | не более 10 минут |
| **Климатические условия эксплуатации** | |
| диапазон рабочих температур | от минус 10 °С до плюс 40 °С |
| относительная влажность воздуха | 93%, при температуре +25 °С |

**Дополнительные изображения**

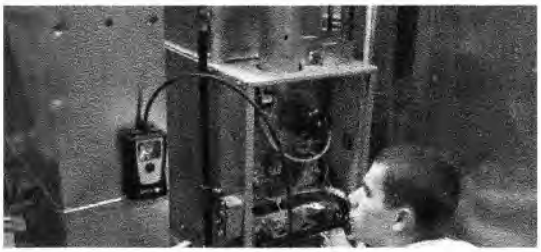
*Телевизионное досмотровое устройство «Поиск-ТВ» в сложенном состоянии*

*Телевизионное досмотровое устройство «Поиск-ТВ» в разложенном состоянии*

*Телевизионное досмотровое устройство «Поиск-ТВ» преодоление межоконного расстояния для визуализации помещения*

## «ЭТВ07» – телевизионный эндоскоп

Новый телевизионный эндоскоп значительно превосходит по техническим характеристикам предшественника. Существенно уменьшены габариты прибора и упрощена работа с ним. Корпус выполнен из высокопрочного пластика, ос-



нащен встроенным источником питания и осветительным блоком. Эндоскоп имеет видеовыход, что позволяет подключаться к внешним мониторам. Регулировка положения дистального конца производится в двух плоскостях.

### Гибкие технические эндоскопы со встроенной автономной светодиодной подсветкой серии ЭТА

Гибкий технический эндоскоп со встроенной автономной светодиодной подсветкой серии «ЭТА» является универсальным досмотровым устройством, обеспечивает быстрый визуальный контроль объектов, имеющих сложную геометрию и объектов, к которым невозможен прямой доступ. Очень прост в эксплуатации.

### Эндоскоп телевизионный гибкий «ЭТВЦ»

Изделие предназначено для визуального контроля в нестационарных условиях неосвещенных мест внутренних полостей, отверстий, труб и другого труднодоступного пространства с применением телевизионного канала регистрации, представления и запоминания изображения.

### Телевизионно-эндоскопическая система «КРОТ-1»

Изделие предназначено для проведения визуального контроля внутренних поверхностей труб в заводских помещениях с целью выявления наличия трещин, расслоений, пятен коррозийного происхождения и других визуально выявляемых дефектов.

### Жесткие технические эндоскопы серии ЭТЖ

Жесткие эндоскопы серии ЭТЖ (бороскопы) предназначены для визуального контроля полостей, щелей, глубоких отверстий или пространств за преградами, к которым возможен прямолинейный доступ через малоразмерные отверстия. Изображение наблюдаемого объекта в бороскопах формируется оптической системой на основе градиентной оптики, благодаря чему формируется изображение с исключительно высоким разрешением. Для освещения наблюдаемого объекта используется волоконно-оптический световод.

### Полужесткие технические эндоскопы со встроенной автономной светодиодной подсветкой серии «ЭТАпж» (с сохранением положения рабочей части)

Полужесткие технические эндоскопы со встроенной автономной светодиодной подсветкой серии «ЭТАпж» (с сохранением положения рабочей части) являются универсальным досмотровым устройством, обеспечивают быстрый визуальный контроль объектов, имеющих сложную геометрию, и объектов, к которым невозможен прямой доступ.

### Гибкие технические эндоскопы с дистальным концом серии «ЭТГ»

Эндоскопы имеют гибкую рабочую часть с управляемым (дистальным) концом. Длина дистального конца не превышает 35 мм. Управление дистальным концом осуществляется в одной плоскости в пределах ±180°. Для передачи изображения и подсветки наблюдаемых объектов используется гибкий оптоволоконный жгут.

## 5.1.2. Ручные металлодетекторы

### Металлодетектор Garrett SuperWand,

предназначенный для ручного досмотра, может применяться при досмотре людей, багажа и т. п. с целью обнаружения предметов из металла. Металлодетектор дает возможность

выявлять цветные и черные металлы. Специалисты нашего сайта тестировали прибор, результаты тестов подтвердили, что благодаря своеобразному дизайну катушки прибор имеет хорошую чувствительность, не зависящую от угла расположения к сканирующей штанге. Это делает досмотр легким, при этом вероятность обнаружения скрытых металлических предметов значительно возрастает.

Обнаружение металла индицируется при помощи звука, вибрации (что дает возможность проводить досмотр, не привлекая внимания окружающих), а также светодиодного индикатора.

**Особенности металлодетектора:**

- сканирующая штанга имеет круговую зону чувствительности по всей ее длине;
- выявление металлических предметов торцом детектора;
- чувствительность настраивается автоматически;
- индикация тревоги: световая, звуковая, вибрационная;
- заряд батареи контролируется автоматически;
- корпус изготовлен из ударопрочного материала;
- имеет небольшой вес и защитное покрытие корпуса.

**Super Wand выявляет:**

- пистолет среднего размера — с расстояния 23 см;
- нож карманный большой — с расстояния 18 см;
- лезвие для бритвы — с расстояния 8 см;
- булавку — с расстояния 2,5 см.

Световые и звуковые индикаторы:

***Зеленый индикатор*** включается каждый раз, когда металлодетектор находится в рабочем режиме.

*Красный индикатор* зажигается при выявлении металла.

***Желтый индикатор*** зажигается, в случае если батарея питания разряжена (в этом случае батарею нужно перезарядить или заменить).

***Звуковой индикатор*** подает громкий звуковой сигнал при выявлении металлического предмета.

***Вибросигнал*** срабатывает в тихом режиме при выявлении металлического предмета.

Super Wand выявляет предметы, изготовленные из металла, только в том случае, когда он движется. Для этого нужно провести металлодетектором на расстоянии 5 см от человека (объекта), который подлежит досмотру. В случае обнаружения металла вы ощутите вибрацию, исходящую от металлодетектора, при этом на нем засветится красный индикатор.

При использовании металлодетектора не требуется производить никаких регулировок, так как работа прибора полностью автоматизирована.

Устройство позволяет выявить любые металлы, черные и цветные. При сканировании ног необходимо проводить Super Wand перпендикулярно полу на расстоянии приблизительно 3 – 5 см от него.

**Технические характеристики:**

Частота работы — 93 кГц.
Частота звукового сигнала — 2 кГц.
Питание — батарейки («Крона») 9 В.
Длительность автономной работы без замены батарей — 80 часов.
Режим настройки — автоматический.
Рабочие температуры — от –37 до +70 °С.
Влажность воздуха при работе — до 95% без прямого конденсата.
Габаритные размеры (Ш×Т×Д), см — 8,3×3,2×48,3.
Масса — 450 граммов.

**Комплект поставки:**

– металлодетектор GARRETT Super Wand;
– инструкция по эксплуатации.

## Ручной металлодетектор «TS100»

Представляет собой компактное устройство, предназначенное для обнаружения предметов из цветных и черных металлов. Прибор может быть использован службами, занимающимися обеспечением безопасности, для личного досмотра людей и досмотра багажа. Металлодетектор позволяет обнаруживать предметы, которые могут быть опасны для людей: огнестрельное и холодное оружие, другие объекты из металла. Устройство TS100 также можно эффективно использовать на заводских проходных для пресечения хищений. Одна из особенностей модели — оповещение об обнаружении металлического объекта только в виде вибросигнала.

Предусмотрен чехол, который используется для ношения устройства на поясе. Модель обладает противоударными качествами, характеризуется компактностью, легкостью конструкции.

Металлодетектор «TS100» может нормально функционировать в неблагоприятных погодных условиях: в температурном диапазоне от −26 °С до +54 °С и при повышенной влажности. Устойчивость к влиянию окружающей среды делает эту модель идеальной для различных охранных служб в любых условиях.

Металлодетектор использует для питания аккумулятор 9 В. Возможно использование батареек. Уровень потребления энергии достаточно низкий.

**Особенности металлодетектора:**

Оповещение при обнаружении объекта: только вибросигнал.

Широкий температурный диапазон, рекомендованный для работы металлодетектора.

Возможность эксплуатации устройства при высокой влажности воздуха.

Корпус металлодетектора обладает противоударными качествами и водонепроницаемостью.

Высокая точность при идентификации.

Обнаружение металлических предметов по всем возможным направлениям.

Компактность модели.

Удобный чехол позволяет постоянно носить металлодетектор на поясе.

**Характеристики металлодетектора:**

Чувствительность прибора:

монета 1 руб. — 50 мм;

металлическая трубка размерами 20 × 400 мм — 100 мм.

Варианты оповещения при обнаружении — вибросигнал.

Питание металлодетектора — аккумуляторная батарея 9 вольт или батарейка 6F22.

Сигнал, сообщающий о низком заряде батарей, — есть.

Рекомендованный для работы диапазон температур — от −26 °С до +54 °С (рабочий диапазон увеличен).

Допустимая влажность воздуха — от 0% до 98% (рабочий диапазон увеличен).

Подстройка — автоматический режим.

Размеры металлодетектора — 210 × 33 × 45 мм.

Вес модели — 250 г.

**Комплектация:**
- металлодетектор «TS100»;
- чехол для ношения на поясе;
- инструкция по эксплуатации.

### 5.1.3. Индикаторы поля и частотомеры

#### Панорамный индикатор поля RAKSA-100

Панорамный индикатор поля «RAKSA-100» предназначен для поиска и обнаружения в ближней зоне радиопередающих устройств, использующихся для негласного съема информации. Среди них мобильные телефоны всех стандартов, устройства Bluetooth, скрытые видеокамеры с передачей информации по радиоканалу, радиомикрофоны, радиомаяки систем слежения.

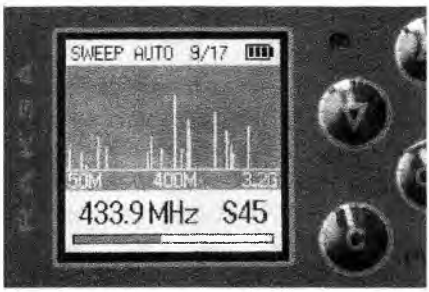
В отличие от широкополосных детекторов (а это практически все индикаторы, представленные на рынке безопасности) «RAKSA-100» обладает частотной селективностью. Это позволяет обнаруживать не только мощные, но и очень слабые сигналы. Кроме того, значительно увеличивается дальность обнаружения радиопередатчиков.

Работая по принципу скоростного сканирующего приемника с широкой полосой канала приема, «RAKSA-100» обнаруживает сигналы с широкополосной и цифровой модуляцией. Но по сравнению с обычными сканирующими приемниками «RAKSA-100» имеет существенно меньшее время реакции на источники радиосигнала.

С помощью панорамного индикатора поля «RAKSA-100» можно получать информацию о частоте радиосигнала не только стандартов GSM900/1800, DECT, Bluetooth, но и CDMA450, который не обнаруживает большинство индикаторов.

В индикаторе поля «RAKSA-100» предусмотрены режимы охраны и поиска.

В охранном режиме прибор в реальном времени без участия оператора отслеживает появление опасных радиосигналов. В этом режиме реализован оригинальный алгоритм адаптации к электромагнитной обстановке, игнорирующий стационарные помехи. Для каждого типа сигнала может быть установлен пороговый уровень. Обнаружение любого из типов сигнала может быть вообще отключено.




В поисковом режиме происходит непрерывное измерение текущего уровня выбранного сигнала и циклическая перестройка по всему диапазону частот. Этот режим используется для локализации источников радиосигналов. На дисплее оператор может наблюдать частоты и уровни всех сигналов, обнаруженных устройством. Результаты отображаются в виде спектрограммы или таблицы.

Индикатор поля «RAKSA-100» имеет банк памяти исключенных и сохраненных каналов. Сохраненные частоты сигналов, обнаруженных прибором, позволяют в дальнейшем быстро на них настроиться. А все сигналы с частотами исключенных каналов в режиме охраны можно удалить из разряда опасных.

**Технические характеристики:**

Диапазон принимаемых частот: 50 МГц — 3 ГГц.
Обнаруживаемые цифровые сигналы: GSM900/1800, DECT, CDMA450, Bluetooth.
Чувствительность: <100 мВ/м.
Динамический диапазон: > 60 дБ.
Ширина канала (полоса пропускания на ПЧ): 1,2 МГц.
Погрешность измерения частоты непрерывного сигнала: ±0,1 МГц.
Время перестройки при отсутствии обнаруженных аналоговых сигналов: < 5 с.
Количество исключаемых/сохраняемых каналов: 200/200.
Дисплей: цветной 1,7" 128×128.
Аккумуляторная батарея: Li-Pol.
Время непрерывной работы от аккумулятора: > 4 ч.
Рабочая температура: 5 — 40 °С.
Температура хранения: — 10 — + 50 °С.
Влажность при 35 °С: < 90 %.
Размеры: 108×68×22 мм.
Вес: 120 г.

## РИЧ-8


Портативный измеритель мощности РИЧ-8 (MFP-8000) — это в полном смысле универсальный прибор, который органично сочетает в себе свойства, присущие сразу нескольким типам измерительных приборов — измерителю мощности, частотомеру, индикатору поля и анализатору сигнатуры.

РИЧ-8 позволяет пользователю в ручном и автоматическом режимах: Определять частоту входного сигнала в диапазоне частот от 100 кГц до 8 ГГц. Измерять мощность входного сигнала в диапазоне уровней от минус 60 дБм до плюс 30 дБм. Идентифицировать во входном сигнале наличие признаков протокола обмена данными для сотовой и телефонной систем связи (GSM900/1800/1900, DECT). Автоматически (посредством встроенного интерфейса) настраивать панорамные радиоприемники или другие устройства на измеренную MFP-8000 частоту сигнала. Использовать (встроенные) память прибора, часы и календарь для протоколирования и хранения результатов измерений. Задействовать встроенный интерфейс для организации использования MFP-8000 в качестве измерительного элемента в составе автоматизированных компьютерных систем.

| | |
|---|---|
| Диапазон рабочих частот: | 0,1 – 8000 МГц |
| Вход: | 50 Ом (не более 1 Вт), разъем N-типа |
| Динамический диапазон измерений уровня мощности: | 90 дБм (от – 60 дБм до + 30 дБм) |
| Точность измерения уровня мощности: | ±0,05 дБм |
| Максимальная измеряемая мощность (со встроенным аттенюатором): | 1 Вт |
| Чувствительность: | При измерении частоты: не хуже 13 мВ (25 дБм) в диапазоне 0,1 – 8000 МГц и не хуже 1,2 мВ ( – 45 дБм) в диапазоне 300 – 6000 МГц<br>При измерении мощности: не хуже 0,510 – 8 Вт |
| КСВН: | Не более 1,5 |
| Диапазон рабочих температур: | 0... + 50 °С |
| Питание: | Встроенная литий-ионная батарея 3,6 В емкостью 1,95 А/ч |
| Средний ток потребления: | Не более 250 мА |
| Габариты: | 115 × 70 × 27 мм |

## Оракул

Скоростной поисковый приемник-корелятор SEL SP-81 «Оракул» предназначен для оперативного обнаружения работающих устройств съема акустической информации, использующих радиоканал.

Наличие пассивного акустического корелятора позволяет бесшумно и скрытно выявлять радиоизлучения, модулированные аналоговыми сигналами (радиомикрофоны) в автоматическом режиме без участия оператора. В приемнике предусмотрены два режима работы: *поисковый* — для обнаружения и локализации источников радиоизлучений и *сторожевой* — для непрерывного контроля за радиообстановкой в реальном времени. При обнаружении сигнала индицируется его частота и уровень, а демодулированный сигнал может воспроизводиться через встроенный громкоговоритель. Приемник обнаруживает радиопередатчики с мощностью в антенне 5 мВт на расстоянии не менее 5 м. Время сканирования всего частотного диапазона зависит от помеховой обстановки и составляет в среднем несколько секунд.

Используемый в приборе метод корреляции предназначен для выявления радиомикрофонов и основан на сравнении демодулированного радиосигнала с опорным акустическим, присутствующим в помещении.

Алгоритм, используемый в приемнике «Оракул», основан на вычислении кросскорреляционной функции текущей мощности акустического сигнала, т. е. его огибающей. Это позволяет не учитывать различие формы исследуемого и опорного сигналов, появляющееся из-за резонансных свойств помещения, что существенно повышает достоверность анализа. Для реализации этого алгоритма оптимально подходит именно речевой сигнал, обладающий высоким пик-фактором (т. е. изменением текущей мощности). Кроме того, этот метод позволяет обнаруживать радиопередатчики с закрытым аналоговым каналом, например, с инверсией спектра.

**Отличительные особенности:**

— сторожевой и поисковый режимы работы;
— встроенный пассивный коррелятор.

**Технические характеристики:**

| | |
|---|---|
| Диапазон принимаемых частот: | 20 – 3000 МГц |
| Виды модуляции сигнала: | WFM, NFM, AM, импульсная (PM) |
| Стандарты обнаруживаемых цифровых сигналов | D-AMPS, DECT, GSM 900, GSM 1800, Bluetooth |
| Чувствительность по входу для захвата сигнала в диапазоне частот | 20 – 200 МГц – 80 дБм (23 мкВ);<br>200 – 600 МГц – 70 дБм (71 мкВ);<br>600 – 1000 МГц – 63 дБм (160 мкВ);<br>1000 – 1400 МГц – 56 дБм (360 мкВ);<br>1400 – 1600 МГц – 49 дБм (795 мкВ);<br>1600 – 2500 МГц – 46 дБм (1,2 мВ);<br>2500 – 3000 МГц – 43 дБм (1,6 мВ) |
| Точка компрессии – 1 дБ по входу: | Не менее 3 дБм |
| Динамический диапазон измерителя уровня сигнала | Не менее 70 дБ |
| Время сканирования диапазона | 12 сек |
| Среднее время настройки на один сигнал | 3 сек |
| Среднее время анализа корреляции одного сигнала | 4 сек |
| Количество запоминаемых сигналов | До 999 |
| Количество исключаемых сигналов | До 999 |
| Ток потребления | Не более 120 мА |
| Источник питания | Батарея 9 В или сеть 220 В через адаптер |
| Дальность обнаружения радиопередатчиков с мощностью в антенне 5 мВт | Не менее 5 м |
| Габаритные размеры (без антенны) | 106 × 68 × 32 мм |
| Масса | 250 г |

### Цифровой индикатор поля – частотомер «Оберег»

Цифровой индикатор поля — частотомер SEL SP-71M создан на основе современных цифровых технологий с использованием микропроцессора, поддерживающего алгоритм работы, который обеспечивает практически мгновенное обнаружение в ближней зоне любых радиопередатчиков, интенсивность излучения которых превышает уровень фона на 6 – 12 дБ, а также обнаружение включенных на передачу сотовых телефонов с возможностью распознавания стандартов GSM и DAMPS.


Устройство по использованному корпусу, органам управления и индикации является псевдопейджером и позволяет его обладателю под видом приема пейджерных сообщений получать информацию о наличии в ближней зоне любого устройства с радиоканалом, предназначенного для негласного получения информации, в том числе скрытно включенного сотового телефона.

«Оберег» имеет 3 режима работы: сторожевой, поисковый и настройки параметров.

Отличительные особенности:

- малогабаритность;
- отсутствие внешней антенны;
- реализован алгоритм адаптивного цифрового фильтра для снижения вероятности ложных срабатываний;
- наличие бесшумной индикации (виброзвонок);
- камуфляж (конструктивно выполнен в корпусе пейджера);
- распознавание сигналов GSM и DAMPS.

**Технические характеристики:**

Диапазон частот: 100 — 2800 МГц.

Дальность обнаружения сотовых телефонов: до 20 м.

Дальность обнаружения радиомикрофонов мощностью 5 мВт: до 3 м.

Динамический диапазон индикатора уровня, не менее: 44 дБ.

Виды индикации: виброзвонок, световая, звуковая (отключаемая).

Питание: 1,5 В (батареи ААА).

Время работы в сторожевом режиме: 24 часа.

Время работы в поисковом режиме: 24 часа.

Габариты: 60 × 40 × 18 мм.

### Детектор поля ST 006

Предназначен для обнаружения и локализации в ближней зоне радиоизлучающих специальных технических средств (РСТС) негласного получения информации.

К таким средствам, прежде всего, относят: радиомикрофоны, телефонные радиоретрансляторы, радиостетоскопы, скрытые видеокамеры с передачей информации по радиоканалу, радиомаяки систем слежения за перемещением объектов, сотовые телефоны, радиостанции и радиотелефоны.

**Отличительные особенности:**

- 16-сегментная светодиодная шкала;
- режим акустической обратной связи (акустозавязки);
- идентификация GSM- и DECT-сигналов;
- индикация непрерывного и импульсного вида сигналов;
- контроль состояния батареи питания.

**Технические характеристики:**

Диапазон рабочих частот:

– 30 – 2500 МГц.

Чувствительность по входу, не хуже:

– 30 – 800 МГц: – 56 dBm (0,35 мВ);
– 800 – 1700 МГц: – 50 dBm (0,71 мВ);
– 1700 – 2400 МГц: – 42 dBm (1,8 мВ).

Динамический диапазон индикации: 48 дБ.

Источник питания: аккумуляторная батарея 3,6 В.

Средний потребляемый ток в рабочем режиме, не более: 40 мА.

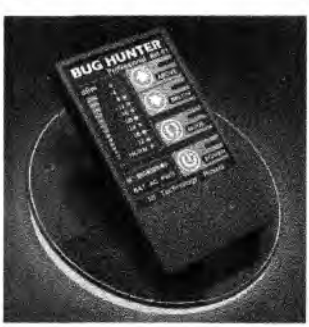
Габариты (без антенны): 85×53×19,5 мм.

Вес: 0,15 кг.

**Комплектация:**

– основной блок: 1;
– телескопическая антенна: 1;
– зарядное устройство: 1;
– техническое описание и инструкция по эксплуатации: 1.

### Индикатор поля Bug Hunter




Предназначен для обнаружения и локализации миниатюрных радиопередатчиков, использующихся для несанкционированного получения информации, а также для беспроводных видеокамер (работающих по радиоканалу), сотовых телефонов и стационарных радиотелефонов.

**Технические характеристики:**

Диапазон рабочих частот: 50 – 3000 МГц.

Чувствительность, не менее: 50 мВ/м.

Динамический диапазон, не менее: 45 дБ.

Режимы работы ВН: поиск, охрана, акустозавязка.

Дальность обнаружения в условиях спокойного радиоэфира, не менее:

- радиопередатчика 5 мВт: 5 м;
- сотового телефона: 50 м.

Габариты: 105 × 58 × 18,5 мм.

### Комплекс радиоконтроля и поиска радиопередающих устройств «Омега»

Комплекс «ОМЕГА» третьего поколения представляет собой аппаратную платформу, предназначенную для анализа электромагнитной обстановки и решения различных задач радиоконтроля.

Позволяет организовать постоянный автоматический мониторинг электромагнитной обстановки в одном или нескольких служебных помещениях с целью выявления вновь появившихся радиосигналов.

Высокая чувствительность радиоприемной части в сочетании с хорошей разрешающей способностью и большой скоростью обзора позволяют оперативно выявлять большинство источников подозрительных радиоизлучений в диапазоне частот от 600 Гц до 18 ГГц.

Основной алгоритм выявления источников радиоизлучений из контролируемой зоны реализован на основе использования метода измерения напряженности поля принимаемого сигнала на пространственно разнесенных антеннах.

Данный алгоритм при контроле нескольких (до 4) помещений позволяет уверенно выявлять работающие в этих помещениях средства прослушивания вне зависимости от используемых в них методов прикрытия информации (кодирование, шифрование, сложные методы модуляции радиосигналов и т. п.).

Широкие возможности по идентификации средств прослушивания предоставляет цифровой векторный анализатор.

Он регистрирует в памяти временные, спектральные и модуляционные характеристики излучений, в том числе импульсных и однократных сигналов, используемых в системах с временным разделением каналов и псевдослучайной перестройкой частоты.

Указанные особенности векторного анализатора позволяют существенно дополнить возможности комплекса в части классифика-

ции выявленных сигналов (по частоте). Программное обеспечение, управляющее комплексом «ОМЕГА», позволяет решить все основные задачи радиоконтроля.

Проведенная модернизация позволила повысить быстродействие, надежность и устойчивость работы комплекса в круглосуточном режиме.

Комплекс ***«ОМЕГА»*** может использоваться для организации как стационарных, так и мобильных постов радиоконтроля.

Основные изменения программного обеспечения направлены на совершенствование алгоритма пространственной локализации источников радиоизлучений и повышения удобства работы пользователя.

Все элементы и узлы комплекса размещены в прочном герметичном кейсе, специально предназначенном для транспортировки сложных электронных приборов.

Аппаратная платформа ***«ОМЕГА»*** допускает дальнейшее расширение возможностей при необходимости решения конкретных задач радиоконтроля.

**Состав комплекта (базовый комплект):**

**«ОМЕГА»** — системный блок в ударопрочном кейсе.

**«АШП»** — антенна широкополосная для установки внутри помещения.

Антенный кабель.

Манипулятор компьютерный типа «мышь».

Головные телефоны.

Кабель питания.

**Основные характеристики:**

| | |
|---|---|
| Диапазон рабочих частот, МГц:<br>базовый комплект<br>с НЧ-преобразователем («ОМЕГА-КС»)<br>с ВЧ-преобразователем («ОМЕГА-К18») | 25 – 3000<br>0,006 – 150<br>2000 – 18000 |
| Скорость обзора, МГц/с | до 500 |
| Разрешение в режиме, кГц:<br>обнаружения анализа | 2<br>0,2 |
| Динамический диапазон по интермодуляции 3-го порядка, дБ | 75 |
| Чувствительность, не хуже, мкВ | 2 |
| Напряжение питания, В | – 200 |
| Габариты, мм | 475 × 480 × 153 |
| Вес, кг | 15 |

## 5.1.4. Анализаторы проводных линий

### Анализатор проводных линий CMA-100

**Назначение**

Усилитель для обследования проводных линий CMA-100 используется для обнаружения и идентификации подслушивающих устройств, передающих информацию по проводным линиям, таким как телефонные линии, компьютерные сети, линии питания, сигнализации и т. д. CMA-100 разработан согласно последним требованиям технической безопасности и гарантирует хорошие результаты обнаружения во многих ситуациях.

**Особенности:**

Имеет встроенный AC/DC-вольтметр, селективные звуковые фильтры с широким динамическим диапазоном.

Сбалансированный вход с высоким сопротивлением обеспечивает гарантированное подключение к подозрительной проводной линии. CMA-100 также обеспечивает напряжение смещения, настраиваемое между −15 В и +15 В, которое используется для активации возможных приборов, которые чувствительны к току или к напряжению. Генератор напряжения смещения соответствует параметрам большинства линий. Все эти функции используют сложную автоматическую схему усиления, что позволяет данному прибору превосходить по характеристикам большинство аудиоусилителей.

**Технические характеристики:**

Входное сопротивление: 50 кОм сбалансированное.
Диапазон АРУ: >75 dB.
Напряжение входа: 10 В р-р.
Автоаттенюатор предусилителя: 0−20 dB (с индикатором перегрузки).
Автоматический контроль мощности усиления: −20 до +120 dB (включая аттенюатор предусилителя).
Ручной контроль мощности усиления: 0, 25, 50, 75, 100 dB.
Контроль мощности усиления в наушниках: 0−15 dB.
Максимальная мощность усиления: 115 dB в ручном режиме, 120 dB в автоматическом режиме.

Частотный диапазон: 100 Гц — 15 кГц.
Высокочастотный фильтр: 300 Гц — 20 кГц.
Низкочастотный фильтр: 100 Гц — 3 кГц.
Полосовой фильтр: 300 Гц — 3 кГц.
Аудиовыход для наушников.
Линейный аудиовыход: 600 Ом.
Контроль напряжения смещения: 0 до +/−15В постоянного тока, 5 мА максимум (защита от перегрузки, входное сопротивление снижается до 3 мОм при активации напряжения смещения).
Цифровой вольтметр: 3,5 значения, автоустановка нуля, автополярность, +/− 199,9 В AC/DC.
Индикатор включения/низкого заряда батареи.
Батарея: 9 В алкалиновая (4 − 7 часов время работы).
Максимальное входное напряжение: 250 В AC/DC.
Внутреннее сопротивление входа: >10 Мом.
Размер: 184,4 × 69,8 × 44,5 мм.
Вес: 343 г.

## Цифровой анализатор проводных и телефонных линий TALAN

**Назначение, технические характеристики**

Анализ, проверка и тестирование проводных линий на наличие устройств негласного съема информации.

**Анализатор спектра:**

Двойного преобразования, приемник с супергетеродином.
Диапазон частот: 10 кГц — 85 МГц.
Скорость сканирования: 2 с.
Шаг: 10 кГц.
Полоса пропускания: 12 кГц.
Чувствительность: − 120 dBm.
Широкополосный детектор:
Диапазон частот (антенный вход): 100 кГц — 8 ГГц.
Диапазон частот (тест линии):
500 кГц — 750 МГц.
Чувствительность: 65 dBm.

**Цифровой мультиметр**

Диапазон: автодиапазон.
Скорость отклика: 500 мс.
Напряжение переменное/постоянное: 0 − 400 В, 0 − 250 В.
Сопротивление: 0 − 400 Мом.
Емкость: 4 нФ — 400 мкФ.

**Генератор напряжения смещения**
Оптически изолированный, прямое цифровое управление.
Максимальное выходное напряжение: ± 80 VDC.
Модуляция (в будущем): синус, «пила», меандр, трапеция.
Частота до 300 Гц.

**Аудио**
Оптически изолированный широкополосный вход.
Полоса 10 МГц.
Номинальная чувствительность: 40 дБ.
Усиление: до 70 дБ общего усиления системы.
АРУ: цифровая.
Фильтр: аналоговый полосовой фильтр.

**Питание**
Напряжение питания: 100 – 240 В, 50 – 60 Гц.
Встроенная батарея литий-ионная, продолжительность работы 4 – 6 ч.

**Габариты и вес**
Размер: 24,1 × 30,5 × 5,0 см.
Вес с батареей: 2,7 кг.
Габариты кейса: 15,9 × 37,8 × 47,0 см.
Вес кейса с прибором: 5,2 кг.
Диапазон рабочих температур: от – 40 °С до + 60 °С.

## Многофункциональный поисковый прибор ST-032

ST-032 предназначен для проведения мероприятий по обнаружению и локализации специальных технических средств негласного получения информации, для выявления естественных и искусственно созданных каналов утечки информации, а также для контроля качества защиты информации. Представляет собой модификацию модели ST-031 «ПИРАНЬЯ». Отличается компактным исполнением и простотой эксплуатации.

**ST-032 имеет следующие режимы работы:**

- высокочастотный детектор-частотомер:

  - идентификация сигналов GSM и DECT;
  - дифференциальный режим;
  - управление сканирующим приемником;
- сканирующий анализатор проводных линий;
- детектор инфракрасных излучений;
- детектор низкочастотных магнитных полей;
- дифференциальный низкочастотный усилитель;
- виброакустический преобразователь;
- акустический преобразователь.

Информация отображается на графическом ЖКИ-дисплее. Акустический контроль осуществляется посредством головных телефонов либо через встроенный громкоговоритель. Питание осуществляется от одной батареи типа АА или от прилагаемого в комплекте блока питания. Для переноски и хранения используется специальная сумка, приспособленная для компактной и удобной укладки всех элементов комплекта.

**Дополнительные возможности:**

для замены программного обеспечения (новые версии, дополнительные возможности) пользователю достаточно подключить ST-032 к своему компьютеру (через последовательный порт) и с сайта производителя, в автоматическом режиме, перепрограммировать прибор.

**Высокочастотный детектор-частотомер**

Диапазон рабочих частот: 30 – 2500 МГц.
Чувствительность: <1 мВ (30 – 1000 МГц); <4 мВ (1000 – 1800 МГц).
Динамический диапазон: 63 дБ.
Чувствительность частотомера: <15 мВ (100 – 1200 МГц).
Точность измерения частоты: ±0,01 МГц.

**Сканирующий анализатор проводных линий**

Диапазон сканирования: 0,05 – 9 МГц.
Чувствительность: при с/ш 10 дБ: <1 мВ.
Полоса пропускания: 10 кГц.
Режим детектирования: АМ, ЧМ.
Допустимое напряжение в сети: 600 В.

**Детектор ИК-излучения**

Спектральный диапазон: 770 – 1000 нм.
Полоса частот детектирования: 0,3 – 300 кГц.

Пороговая чувствительность: <10 – 13 Вт/Гц½.
Полоса частот: 5 МГц.

**Детектор НЧ магнитного поля**
Диапазон частот: 0,5 – 300 кГц.
Пороговая чувствительность:10 – 11 Тл/Гц½.

**Виброакустический преобразователь**
Чувствительность: 1 В × сек²/м.
Диапазон частот: 0,3 – 6 кГц.
Пороговая чувствительность: 5 × 10 – 6 м/с².

**Акустический преобразователь**
Чувствительность: >5 мВ/Па.
Диапазон частот: 0,3 – 8 кГц.
Уровень эквивалентного звукового давления, обусловленный собственными шумами: <40 дБ.

**Дифференциальный низкочастотный усилитель**
Динамический диапазон: 60 дБ.
Входное сопротивление: 200 Ком.
Коэффициент ослабления синфазной помехи: > 60 дБ.
Приведенное ко входу напряжение шумов: < 20 мкВ.
Диапазон частот: 0,2 – 15 КГц.
Максимально допустимое входное напряжение: 70 В.

**Звуковой тракт**
Диапазон частот: 0,2 – 20 кГц.
Диапазон частот встроенного излучателя: 0,5 – 5 кГц.
Максимальная выходная мощность встроенного излучателя: 100 мВт.

**Питание**
Напряжение питания: 1,5/220 В.
Средний потребляемый ток: <100 мА.

**Габариты**
Основной блок: 157 × 62 × 28 мм.
Сумка.

**Вес**
Основной блок: 0,25 кг.
Брутто: <1 кг.

## 5.1.5. Нелинейные локаторы

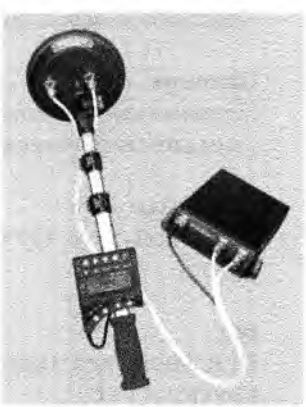
### ЛОРНЕТ 24

«ЛОРНЕТ 24» используется при проведении оперативно-поисковых работ в помещениях, в автомашинах, досмотре людей и бандеролей, обнаруживает технические средства и устройства, имеющие в своем составе полупроводниковые компоненты.

Оснащен системой автоматического выбора частот и может автоматически отстраиваться от сосредоточенных помех (по критерию минимального шума в канале приема 2-й гармоники).

- Вид зондирующего сигнала: импульсный, непрерывный.
- Мощность сигнала импульсного (скважность 50)/непрерывного: 10/1 Вт.
- Чувствительность: не хуже — 108 дБм (при отн. сигнал/шум = 10).
- Частота сигнала: 2400 — 2483 МГц.
- Динамический диапазон: более 80 дБ.
- Время работы от встроенного аккумулятора при макс. мощности зондирующего сигнала (импульсный/непрер.): не менее 3/1 ч.
- Размеры в транспортном/рабочем положении: 23 × 10 × 5,5/39 × × 10 × 4 см.
- Полный вес изделия в рабочем состоянии: менее 700 г.

### NR 900 EM



NR 900 EM предназначен для поиска электронных устройств, содержащих полупроводниковые компоненты. Прибор применяется для обследования любых ограждающих строительных конструкций, стен, мебели, предметов интерьера и выявления электронных устройств негласного получения информации (радиомикрофонов, микрофонных усилителей, диктофонов и т. п.), в различных режимах работы: в режиме передачи, в выключенном или в <сторожевом> режиме (для устройств с дистанционным управлением).

**Передатчик**

- Частота: 860 + 2 МГц.
- Выходная импульсная мощность: не менее 200 Вт [+53 dBm] (средняя мощность не более 0,1 Вт [+ 20 dBm]).
- Диапазон регулировки мощности: (8+ 2 dB).
- Вид модуляции зондирующего сигнала: амплитудно-импульсный (скважность 2350).
- Частота: 1720 МГц — 2580 МГц.
- Чувствительность (с учетом цифровой обработки): не хуже −123 дБ/Вт (− 93 dBm) [при соотношении с/ш 6 дБ].
- Ступенчатое ослабление входных сигналов: −10, −20, −30, −40, −50 dB.

**Антенна**

- Тип поляризации: круговая.
- Коэффициент эллиптичности: не хуже 0,75.
- Коэффициент усиления:
  — приемной антенны: не менее 6 дБ;
  — передающей антенны: не менее 8 дБ.
- Ширина главного лепестка диаграммы направленности: не более 40°.
- Уровень задних лепестков диаграммы направленности: не более −15 дБ.

**Индикация**

Звуковая: тональный сигнал (212 Гц).

Визуальная: 4-строчный ЖК-индикатор.

Динамический диапазон индикатора уровней сигналов: 30 дБ.

Отображаемая информация: уровень 2 гармоники (сегментная шкала и цифровое значение), уровень 3 гармоники (сегментная шкала и цифровое значение), разность уровней 2 и 3 гармоники (цифровое значение), текущее значение аттенюатора приемников, индикация значения выходной мощности, индикация подключения телефонов к приемнику на 2 или 3 гармонике, символ режима подавления GSM, напряжение аккумулятора.

### 5.1.6. Обнаружители скрытых видеокамер

### «Гранат» – прибор обнаружения скрытых видеокамер

**Назначение**

Простой и очень эффективный прибор для поиска скрытых видеокамер. Позволяет обнаружить ка-

меры, спрятанные в стене или мебели, в пуговице или значке, в портфеле или сумке, с обычным объективом или микрообъективом (типа pin-hole), включенные или выключенные, передающие изображение по проводам или по радиоканалу. Легкий и компактный, «Гранат» поможет обследовать любое помещение: офис, сауну, кабинет врача или гостиничный номер и защитить вас от шантажа, промышленного шпионажа, слежки супруга и других неприятных сюрпризов.

**Особенности**

В основу принципа работы изделия «Гранат» положен эффект световозвращения, заключающийся в способности оптических объектов отражать зондирующее излучение в обратном направлении под углом, близким к углу его падения. Источником зондирующего излучения служат мигающие ИК-диоды. Отраженный сигнал воспринимается визуально через окно с фильтром на приборе.

**Базовый комплект поставки:**

Прибор «Гранат».
Элементы питания типоразмера ААА.
Штатная упаковка (картонная коробка).
Руководство по эксплуатации.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Расстояние обнаружения зрачков ССВ диаметром 1 мм | |
| Минимальное, м | 0,2 |
| Максимальное, м | 10 |
| Поле подсветки (Г × В) | 2° × 6° |
| Время непрерывной работы от аккумулятора не менее, ч | 5 |
| Диапазон рабочих температур: | −10° С... + 50° С |
| Размеры, мм | 115 × 32 × 18 |
| Масса, г | 60 |

**Дополнительные изображения**

*Пример обнаружения скрытой видеокамеры прибором «Гранат»*

## Аппаратура обнаружения скрытых телевизионных систем наблюдения «Антисвид-2»

### Назначение

Для поиска и визуализации местоположения портативных систем скрытого видеонаблюдения (ССВ), закамуфлированных в предметах интерьера и бытовых изделиях личного пользования, работающих или отключенных малогабаритных видеокамер в различных условиях освещения. Прибор позволяет вести работу как в полной темноте, так и в условиях интенсивной фоновой засветки. Позволяет обнаруживать скрытые оптико-электронные устройства (СОЭУ) за такими преградами, как стекло (в том числе тонированное), оргстекло, полупрозрачные зеркала. Следует отметить, что угол обнаружения СОЭУ равен углу поля зрения самих СОЭУ. В основу принципа работы прибора положен эффект световозвращения, заключающийся в способности оптических объектов отражать зондирующее излучение в обратном направлении под углом, близким к углу его падения.

### Комплект поставки

Прибор «Антисвид-2».
Руководство по эксплуатации.
Аккумуляторная батарея.
Зарядное устройство.
Сверхпрочный транспортный кейс (упаковка-укладка).

### Технические характеристики

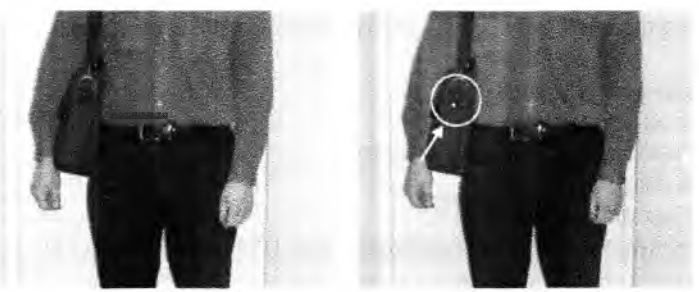
| Наименование | Значение |
|---|---|
| Расстояние обнаружения зрачков ССВ диаметром 1 мм: | |
| минимальное, м | 1 |
| максимальное, м | 15 |
| Максимальный угол пеленга видеокамер | Соответствует углу поля зрения самих видеокамер |
| Поле зрения приемного канала (Г×В) | 6°×8° |
| Поле лазерной подсветки (Г×В) | 2°×6° |
| Время непрерывной работы от аккумулятора не менее | 5 ч |
| Электропитание прибора: | |
| Мощность не более | 5 Вт |

| | |
|---|---|
| аккумулятора NP-F770 | +7 В, 4400 мА час |
| сетевого адаптера | 220 В/50 Гц-12 В; 1,5 А |
| Габаритные размеры прибора без ЖК-монитора, не более, мм | 240 × 160 × 80 |
| Масса прибора без ЖК-монитора, с аккумулятором, не более, кг | 1,6 |

**Дополнительные изображения**

*Обнаружена видеокамера размером менее 1 мм*

*Обнаружена видеокамера размером менее 1 мм, дистанция 4 м*



*Пример обнаружения микровидеокамеры, закамуфлированной в сумку: а) блок сканирования выключен; б) блок сканирования включен*

*Пример обнаружения микровидеокамеры с объективом типа «pinhole» в различных условиях освещения прибором «Антисвид». E~0,001 люкс, дистанция 6 м*

### Обнаружитель скрытых видеокамер «Алмаз»

Прибор предназначен для обнаружения скрытых микровидеокамер при проведении поисковых мероприятий в помещениях на дальности до 10 метров. Обнаружение не зависит от состояния камер (включено/выключено). Также позволяет обнаруживать утерянные (оброненные) драгоценные камни (алмазы, бриллианты). Обнаружение происходит при нахождении «Алмаза» в поле зрения искомой видеокамеры. «Алмаз» обнаруживает скрытые видеокамеры в любом виде камуфляжа и в любом состоянии: в стенах, потолках, сумках, в различных упаковках, внутри электромагнитного экрана — даже когда камера выключена.

**Технические характеристики:**

- Масса: 200 г.
- Габаритные размеры: 50 × 50 × 100 мм.
- Источник электропитания: литиевая батарея напряжением 3 В.
- Время непрерывной работы от заряженной батареи: до 30 часов.
- Выходная мощность лазера: менее 10 мВт.

## 5.1.7. Тепловизоры

### «Testo 880» – измерительный тепловизор

**Назначение**


Человеческий глаз не способен увидеть инфракрасное излучение. Однако все объекты, температура которых выше абсолютного нуля, приблизительно —273 градуса по Цельсию, излучают инфракрасные волны.

Тепловизоры могут конвертировать инфракрасное излучение в электрические сигналы и таким образом представлять их визуально. Благодаря превосходному качеству снимков Testo 880 можно увидеть даже небольшую разницу в температуре.

Сменная оптика обеспечивает уверенность в том, что нужный сегмент изображе-

ния всегда виден, обеспечивая гибкий подход при решении различных измерительных задач. Встроенная цифровая камера значительно облегчает документирование.

Testo 880 позволяет в режиме реального времени локализовать точки, где существует риск возникновения плесени, что является уникальным в сфере термографии зданий.

Термография используется в строительстве, промышленности и других областях, где она необходима.

**Особенности**

Testo 880-1 — базовый прибор для быстрого обнаружения неполадок и контроля качества.

Высококачественный широкоугольный объектив с углом 32° с оптикой F1.

Частота обновления изображения 9 Hz.

Детектор 160×120, интерполируемый до 320×240 пикселей.

NETD < 0,1 °C.

Ручной фокус.

Минимальное фокусное расстояние — 10 см.

Устройство хранения данных — карта памяти SD, 1 Гб, прибл. на 800 — 1000 снимков.

**Включено в поставку:**

ПО с функцией создания отчетов.

USB-канал.

Литиево-ионный аккумулятор.

Высококачественный, прочный кейс.

**Testo 880-2** — профессиональный тепловизор с расширенными функциями анализа и возможностью установки сменного телеобъектива.

**Дополнительные функции по сравнению с Testo 880-1:**

Возможность установки сменного объектива.

Отображения распределения поверхностной влажности 33 Гц версия (по запросу).

Стекло для защиты объектива.

**Testo 880-3** — тепловизор для экспертов для полного анализа и документирования реальных изображений зданий, электрических систем и машин.

**Дополнительные функции для Testo 880-3:**
Встроенная цифровая камера с мощной LED-подсветкой.
Динамический моторизированный фокус.
Отображение распределения поверхностной влажности в режиме реального времени с беспроводным зондом (опция).

**Дополнительный комплект поставки**
Защитный фильтр для объектива.
Телеобъектив.
Дополнительный аккумулятор.
Быстродействующее зарядное устройство.
Солнцезащитная бленда для дисплея.
Измеритель влажности.

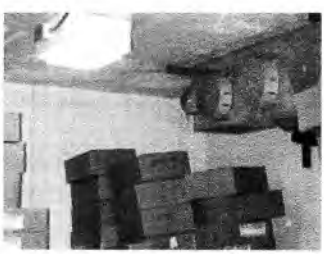
**Технические характеристики**

| **Название** | **Значение** | | |
|---|---|---|---|
| Характеристики изображений | **Testo 880-1** | **Testo 880-2** | **Testo 880-3** |
| **Инфракрасное** | | | |
| Оптическое поле зрения/ мин. фокус, расстояние | 32° × 24° / 0,1 м (стандартный объектив), 12° × 9°/0,6 м (телеобъектив) | | |
| Температурная чувствительность (NETD) | <0,1 °C про 30 °C | | |
| Пространственное разрешение | 3,5 мрад — стандартный объектив, 1,3 мрад (телеобъектив) | | |
| Частота обновления кадров | 9 Гц | 9 Гц вне, 33 Гц в пределах ЕС | |
| Фокусировка | Ручная | Ручная + моторизированная | |
| Тип детектора | FPA 160 × 120 пикселей, a.Si | | |
| Спектральный диапазон | 8 до 14 — µм | | |
| **Визуальное** | | | |
| Оптическое поле зрения/мин. фокус, расстояние | | | 33,2° × 25,2°/0,4м |
| Размер изображения | | | 640 × 480 пикс. |
| Частота обновления кадров | | | 8 – 15 Гц |
| **Представление изображения** | | | |
| Дисплей | 3,5" LCD с 320 × 240 пикс. | | |
| Возможность отображения | Только ИК-изображение | | 1. ИК-изобр.<br>2. Реальн. изобр.<br>3. ИК + реальное |

| | | | |
|---|---|---|---|
| Видеовыход | USB2 | | |
| Потоковое видео | 9 Гц | 25 Гц | |
| Цветовая палитра | 8 вариантов | | |
| **Измерение** | | | |
| Температурный диапазон | −20 +100 °C; 0 +350 °C (переключаемый) | | |
| Погрешность | ±2 °C, ±2% от измеряемого значения | | |
| Минимальный диаметр точки измерения | 3×3 пикселя, стандартно 10 мм при 1 м (стандартный объектив), стандартно 4 мм при 1 м (телеобъектив) | | |
| Время включения | 40 с | | |
| Измерение влажности и температура воздуха с беспроводным зондом (опция) | | | 0 до 100 %ОВ/ −20 до +100 °C −20 до +70 °C (температура воздуха NTC) |
| Погрешность беспроводного зонда | | | ±2 %ОВ/ ±0,5 °C (температура воздуха) |
| Функции измерений | Стандартное измерение (1-точечное), 2-точечное измерение | | |
| | | Расчет точки росы через ручной взвод, значения влажности, расчет значения поверхностной влажности | |
| | | | Опциональное измерение влажности с беспроводным зондом |
| Температурная компенсация отражения | Ручная | | |
| Настройка коэффициента излучения | 9 материалов памяти, из них один задается пользователем (0,01 — 1,0) | | |
| **Хранение изображений** | | | |
| Формат файлов | .bmt; возможность экспорта в bmp,.jpg,.csv | | |
| Устройство хранения данных | Карта памяти SD | | |
| Объем памяти | 1 Гбайт (приблиз. 800 — 1000 изображений) | | |
| **Оптика** | | | |
| Стандартный объектив (32°) | Есть | | |
| Телеобъектив (12») | Нет | Есть, опционально | |

| Лазерный целеуказатель точки измерения | |
|---|---|
| Классификация лазера | 635 нм, класс 2 |
| Электропитание | |
| Тип аккумулятора | Быстрая зарядка, Li-ion аккумулятор, заменяемый по месту замера |
| Время работы | Приблиз. 5 ч. При 20 °C |
| Возможность зарядки | В приборе/в зарядном устройстве (опция) |
| Работа от блока питания | Да |
| Выходное напряжение | 5 В |
| **Условия окружающей среды** | |
| Диапазон рабочих температур | −15 + 40 °C |
| Температура хранения | −30 + 60 °C |
| Влажность воздуха | 20 % до 80 % без образования конденсата |
| Класс защиты корпуса | IP54 |
| **Физические характеристики** | |
| Вес | 900 г |
| Габариты | 152 × 106 × 262 мм |
| Крепление к штативу | Да |
| Корпус | ABS |
| **ПО для ПК** | |
| Системные требования | ОС Windows XP (Service Pack 2), Windows Vista |

**Дополнительные изображения**



*Видимый свет*

*Инфракрасный свет. Осветительные приборы и проводка*

## 5.1.8. Рентгеновские установки

### Переносной рентгенотелевизионный комплекс «Flat Scan 27»

**Назначение**

Переносной рентгенотелевизионный комплекс «Flat Scan 27» предназначен для быстрого, радиационно-безопасного рентгенов-

ского обследования внутреннего содержимого различных предметов, багажа, грузов, посылок, транспортных средств с целью обнаружения оружия, наркотиков, взрывных устройств и других запрещенных предметов; поиска скрытых систем съема аудио- и видеоинформации в помещениях (стены, мебель, оргтехника, средства связи). Может быть использован для дефектоскопии и решения задач техногенной безопасности в полевых условиях.

Данный комплекс используют таможенные службы, службы безопасности, оперативные службы ФСБ, ФСО, МВД, ФСКН России и другие структуры, занимающиеся обеспечением безопасности. Оценка подозрительных предметов, находящихся в общественных местах (обнаружения оружия, взрывных устройств и т. п.). Проведение мобильных таможенных проверок.

Проверка крупногабаритных предметов, которые не могут быть сканированы стационарными рентгено-телевизионными комплексами. Безопасное промышленное использование в области неразрушающего контроля (например, контроль сварных соединений).

**Особенности**

- Рентгеновский аппарат со встроенной аккумуляторной батареей.
- Управление напряжением и током через портативный компьютер.
- Снабжен тонким, плоским рентгенооптическим преобразователем (50 мм в толщину), способным сканировать предметы, находящиеся в труднодоступных местах.
- Обеспечивает высокое качество передачи изображения.
- Обладает высокой способностью проникновения (вплоть до 30 мм стали на 120 кВ, 1мА).
- Обладает возможностью сканирования на разных скоростях.
- Прост и удобен в использовании.

**Комплект поставки комплекса «Flat Scan 27»:**

- Высококачественный прочный автономный рентгенооптический преобразователь сканирующего типа.
- Портативный компьютер.
- Портативный рентгеновский аппарат CP120 или CP160.

**Опции**

- Разрешение: 200 микрон (2048 пикселей) или 400 микрон (1024 пикселей).
- Рентгеновский аппарат: 160 кВ; 0,5 мА.
- Трансляционные беспроводные усилители.
- Беспроводное соединение.
- Станция изображения: Toughbook.
- Многофункциональное зарядное устройство для всего комплекта.
- Штатив.
- Сумки для транспортировки рентгенооптического преобразователя, рентгеновского аппарата и портативного компьютера.

**Технические характеристики**

| Наименование | Значение | |
|---|---|---|
| Разрешение | 800 микрон (512 пикселей) | |
| Проникновение по стали (CP120) | Не менее 25 мм | |
| Соединение | Беспроводное | |
| Питание | Аккумуляторные батареи | |
| Количество снимков на полностью заряженном аккумуляторе | не менее 80 снимков | |
| **Рентгенооптический преобразователь** | | |
| Тип | Linear PIN diode array | |
| Разрешение | 800 микрон (512 пикселей) | |
| Динамический радиус действия | 4096 (12-bit) | |
| Сканируемая площадь | 560 × 400 мм | |
| Скорость линейного сканирования | от 6 м/мин до 0,5 м/мин | |
| **Габаритные характеристики рентгенооптического преобразователя** | | |
| Внешние размеры | 720 × 623 × 50 мм | |
| Вес | менее 8 кг | |
| **Приемник получаемого изображения** | | |
| Тип | Прочный портативный компьютер | |
| **Климатические условия** | | |
| Температура эксплуатации | 0 °C – +40 °C | |
| Температура хранения (при относительной влажности: не более 95%) | –40 °C – +80 °C | |
| **Технические характеристики генератора рентгеновских лучей** | | |
| **Наименование** | **CP120** | **CP160** |
| Тип | Постоянный потенциал | |
| Доза рентгеновских лучей, 1 фут | 1000 μSV/s | 4000 μSV/s |

| | | |
|---|---|---|
| Максимальная мощность /1бат: | 5 – 6 мин постоянной генерации рентгеновских лучей (вплоть до 120 изображений с 3-секундной экспозицией) | |
| Максимум кВ | 120 кВ (регул. кВ: 40 – 120) | 160 кВ (регул. кВ: 60 – 160) |
| Максимум мА | 1,5 мА, регулируется с шагом 0,5 мА между 40 и 80 кВ, 1 мА между 81 и 120 кВ | 1,5 мА, регулируется с шагом 0,5 мА между 60 и 110 кВ, 1 м А между 111 и 160 кВ |
| Время экспозиции: | Регулируется от 1 сек до 99 сек | |
| Время предупреждения | Регулируется от 0 сек до 99 сек | |
| Максимальное проникновение | 30 мм стали | 40 мм стали |
| Гарантированное проникновение | 25 мм стали | 35 мм стали |
| Размер фокусного пятна | 0,25 × 0,50 мм | 0,20 × 0,40 мм |
| Ресурс трубки | Неограничен | |
| 2 батареи (1 запасная) | Никель-кадмиевые 36В; 600 мА/час | |
| Вес | 6,5 кг | 7 кг |
| Угол луча | 65° × 52° | 60° × 40° |

**Программное обеспечение**

Оператор может выбрать все следующие стандартные операции процессов: реверсировать черный и белый цвета, включить псевдоцвет, увеличить изображение, изменить контраст, изменять параметры CP120 и CP160 для обеспечения максимально глубокого проникновения.

**Двойная энергия**

Благодаря особой конструкции рентгеновских аппаратов СР120 и СР160 реализована опциональная программа идентификации материалов на основе алгоритма двойной энергии. Эта программа обеспечивает выделение различными цветами на рентгенооптическом изображении, представленном на экране портативного компьютера, органические (например, взрывчатку и наркотики) и неорганические (металлы) субстанции, находящиеся в подозрительных предметах багажа.

## Рентгеновский сканер скрытых полостей «Ватсон»

**Назначение**

Рентгеновский сканер скрытых полостей «Ватсон» предназначен для поиска оружия, наркотиков, контрабандных вложений в транспортных средствах. Может использоваться для поиска закладок в помещениях (стены, мебель, двери).

Досмотр полостей с односторонним доступом — 10 секунд на проверку колеса.

**Особенности**

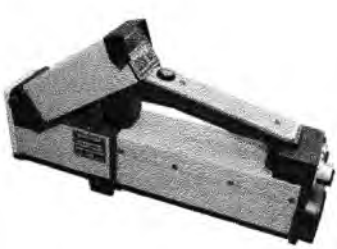
Питание прибора осуществляется от сетевого адаптера или аккумуляторного блока. Во время досмотра сканер и аккумуляторный блок располагаются на поясе оператора. При транспортировке и хранении комплект оборудования размещается в легкой армированной сумке. Широкий динамический диапазон позволяет разделять вложения по объему и плотности.

Возможность радиационного мониторинга. Высокая скорость досмотра.

Сканирование в абсолютном и относительном режимах. Используется рентгеновский источник излучения. Радиационная безопасность.

**Базовый комплект поставки:**

Сканирующее устройство.
Устройство питания (аккумуляторный блок 2А).
Зарядное устройство.
Сетевой адаптер.
Пояс с креплением.
Футляр.
Паспорт.
Запасные предохранители (2 шт.).



**Технические характеристики**

| Наименование | Значение |
|---|---|
| Максимальная толщина преграды, за которой обнаруживается предмет размерами 20×20×20 мм и плотностью 0,5 – 2 г/см$^3$ | |
| дерево | 45 мм |
| алюминий | 10 мм |
| сталь | 1,5 мм |
| Максимальная глубина досмотра | 300 мм |
| Скорость сканирования | 10 см/с |
| Габаритные размеры | 322×172×70 мм |
| **Масса** | |
| Сканер | 2,4 кг |
| Пояс с аккумуляторным блоком | 1,7 кг |
| Диапазон рабочих температур | – 20° ... + 50° С |

**Дополнительные изображения**

*Рентгеновский сканер скрытых полостей «Ватсон» в упаковке-укладке*

## 5.1.9. Сканеры

### Icom IC-R10

Модель ICOM IC-R10 воплотила в себе все современные технологические достижения, что позволило добиться высококачественного приема сигналов всех видов модуляции в диапазоне от коротких волн до СВЧ при сохранении небольших габаритов и веса. Ряд функ-

ций (Voice Scan Control, Real-time fluLJi Band Scope, SIGNAVI) впервые реализован в носимом сканере.

Расширенный набор типов и видов сканирования: каждый из двух основных типов сканирования (программируемое и по каналам памяти) разбит на три вида: сплошное, диапазонное, с автоматической записью частот, по каналам памяти, по видам модуляции, по банкам памяти.

Новая функция SIGNAVI позволяет в несколько раз увеличить реальную скорость сканирования. При сканировании в режиме FM используется дополнительный приемный контур, который продолжает сканирование при нахождении основным приемником сигнала, таким образом, основной приемник сканирует скачками, только по занятым каналам. Величина скачков составляет до 5 шагов настройки, но не более 100 кГц.

| **Технические характеристики** | **ICOM IC-R10** | | | |
|---|---|---|---|---|
| Диапазон частот, МГц | 0.5...1300 | | | |
| Виды модуляции | SSB, AM, CW, FM, WFM | | | |
| Чувствительность, мкВ (AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | FM | 0.5...5 МГц-0.5<br>5...200 МГц-0.32 | 200...340 МГц-0.45<br>340...700 МГц-0.35 | 700...800 МГц-0.79<br>800...1300 МГц-0.5 |
| | WFM | 75...200 МГц-1.0<br>200...240 МГц-2.2 | 340...700 МГц-1.3<br>700...800 МГц-2.0 | 800...900 МГц-1.6 |
| | AM | 0.5...5 МГц-1.6<br>5...200 МГц-1.0 | 200...340 МГц-1.6<br>340...700 МГц-1.4 | 700...800 МГц-2.0<br>800...1300 МГц-1.6 |
| | SSB, CW | 0.5...5 МГц-0.4<br>5...200 МГц-0.25 | 200...340 МГц-0.4<br>340...700 МГц-0.32 | 700...800 МГц-0.63<br>800...1300 МГц-0.4 |
| Количество каналов памяти | 1000 | | | |
| Потребляемый ток max/min, мА | 180 / 38 | | | |
| Диапазон рабочих температур | − 10°... + 50 °C | | | |
| Габариты и вес | 59 × 130 × 32 мм, 310 г | | | |

Компьютерный интерфейс. ICOM IC-R10 может быть подключен к компьютеру для клонирования или управления. Обмен данными осуществляется в разработанном ICOM формате CI−V через дополнительный блок CT-17 и позволяет как считывать данные (частоты, уровень сигнала), так и управлять всеми функциями приемника. Приемник ICOM IC-R10 поддерживается большинством управляющих программ (ARCON, SEDIF и др.).

Для клонирования или программирования памяти требуется программа CS-R10 и кабель OPC-478.

Расширенные функции использования памяти. 1000 каналов памяти разбиты на 18 банков (16 банков по 50 каналов, 2 банка по 100 каналов для автоматической записи частот и каналов пропуска). В каждом канале запоминается частота, вид модуляции (включая ширину полосы), шаг настройки и т. д. Каналам и банкам памяти можно присвоить буквенные имена длиной до 8 символов. Специальная EEPROM память сохраняет информацию даже при севших аккумуляторах. Функция редактирования памяти позволяет производить копирование и вставку содержимого каналов.

Интеллектуальная система поиска голоса. VSC (Voice Scan Control) позволяет пропускать смодулированные и шумовые сигналы.

### Icom IC-R2

IC-R2 — представитель нового поколения сканирующих приемников. Главная его особенность — большие возможности в миниатюрном корпусе.

Широкий диапазон: 0.495 – 1309.995 (разбит на 9 поддиапазонов) с шагом от 5 до 100 кГц.

Виды модуляции: AM, FM, WFM, встроенный декодер тонов CTCSS.

Функции прослушивания приоритетного канала (priority watch) и дуплексных каналов (offset monitor).

Простота в работе. Приемник имеет всего девять кнопок управления. Понятные символы на дисплее позволяют за несколько минут разобраться со всеми функциями.

Компактные размеры. Небольшой плоский корпус удобно ложится в вашу ладонь.

Брызгозащищенное исполнение.

Гибкие возможности сканирования: по всему диапазону, граммированных границах, по каналам памяти.

| Технические характеристики | ICOM IC-R2 |
|---|---|
| Диапазон частот, МГц | 0.495...1309.995 |
| Виды модуляции | AM, FM, WFM |

| Чувствительность, мкВ (AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | FM | WFM | AM |
|---|---|---|---|
| | 1.6...5 МГц-0.4<br>5...30 МГц-0.25<br>30...118 МГц-0.2<br>118...175 МГц-0.18<br>175...470 МГц-0.22<br>470...1000 МГц-0.28<br>1000...1310 МГц-0.45 | 30...118 МГц-0.71<br>175...470 МГц-0.71<br>470...1000 МГц-1.0 | 0.5...5 МГц-1.3<br>5...30 МГц-0.79<br>118...136 МГц-0.63<br>222...247 МГц-0.63<br>247...330 МГц-0.71 |
| Скорость сканирования | до 30 каналов/сек | | |
| Количество каналов памяти | 450 (400 стандартных, 50 границ сканирования) | | |
| Потребляемый ток max/min, мА | 170 / 41 | | |
| Диапазон рабочих температур | −10...+60 °C | | |
| Габариты и вес | 58×86×27 мм, 170 г | | |

## Icom IC-R3

Носимый сканирующий приемник с возможностью просмотра видеоизображений.

Никогда ранее портативный приемник не предоставлял так много информации, как сейчас это может сделать ICOM ICRS. Телевизионное изображение, спектр и многое другое можно увидеть на 2-дюймовом цветном TFT-экране.

Большой 2-дюймовый TFT-дисплей, позволяющий просматривать видеоизображения (PAL B/G, NTSC). Прием как телепрограмм и звука (разнос 4,5 или 5,5 МГц), так и видеоизображений со следящей камеры.

Расширенные функции использования памяти. 450 каналов памяти для удобства использования разбиты на 8 банков по 50 каналов. Один банк из 50 каналов используется для записи границ сканирования.

Автоматический шумоподавитель. Имеется возможность ручного управления шумоподавителем (9 уровней и полное открытие).

Li-ion аккумулятор и зарядное устройство входят в комплект поставки.

| Основные технические характеристики | ICOM IC-R3 | | | |
|---|---|---|---|---|
| Диапазон частот, МГц | 0,495...2450,095 | | | |
| Виды модуляции | FM, AM, WFM, AM-TV, FM-TV | | | |
| Шаг перестройки частоты, кГц | 5, 6.25 | | | |
| Количество каналов | 450 (50×8 банков + 50×1 банк для записи границ сканирования) | | | |
| Диапазон рабочих температур | -10 ... +60 °C | | | |
| Чувствительность, мкВ (при включенном предусилителе; SSB, CW, RTTY, AM — 10дБ S/N; FM, WFM — 12 дБ SINAD) | FM | 0,5...5 МГц-0,5<br>5...200 МГц-0,32 | 200...340 МГц-0,45<br>340...700 МГц-0,35 | 700...800 МГц-0,79<br>800...1300 МГц-0,5 |
| | WFM | 75...200 МГц-1,0<br>200...240 МГц-2,2 | 340...700 МГц-1,3<br>700...800 МГц-2,0 | 800...900 МГц-1,6 |
| | AM | 0,5...5 МГц-1,6<br>5...200 МГц-1,0 | 200...340 МГц-1,6<br>340...700 МГц-1,4 | 700...800 МГц-2,0<br>800...1300 МГц-1,6 |
| | SSB, CW | 0,5...5 МГц-0,4<br>5...200 МГц-0,25 | 200...340 МГц-0,4<br>340...700 МГц-0,32 | 700...800 МГц-0,63<br>800...1300 МГц-0,4 |
| Напряжение пит. / Ток потр. | 3,6...6,3 В /0,21 А (ном. громк., LCD — выкл.),<br>0,73 А (LCD — вкл.) | | | |
| Габариты и вес | 61×120×33 мм, 0.3 кг | | | |

## Icom IC-R5

IC-R5 — представитель нового поколения сканирующих приемников, дальнейшее развитие популярной модели IC-R2. Главные его особенности — большие возможности в миниатюрном корпусе при невысокой цене. Широкий диапазон: 0.15 — 1309.995 МГц (разбит на 9 поддиапазонов) с шагом от 5 до 100 кГц.

Виды модуляции: AM, FM, WFM, встроенный декодер тонов CTCSS и DTCS.

Функции прослушивания приоритетного канала (priority watch) и дуплексных каналов (offset monitor).

Простота в работе. Приемник имеет всего девять кнопок управления, понятные символы на дисплее позволяют за несколько минут разобраться со всеми функциями.

Компактные размеры. Плоский корпус небольших размеров удобно ложится в вашу ладонь.

Брызгозащищенное исполнение.

Гибкие возможности сканирования: по всему диапазону, в запрограммированных границах, по каналам памяти.

Автоматический шумоподавитель.

Знакосимвольный дисплей с подсветкой.

До 100 мВт акустической выходной мощности.

Приемник работает от двух элементов питания типа АА.

Разъем для подключения наушника и внешнего источника питания.

Функции клонирования и программирования памяти с компьютера.

| **Технические характеристики** | **ICOM IC-R5** | | |
|---|---|---|---|
| Диапазон частот, МГц | 0.495...1309.995 | | |
| Виды модуляции | AM, FM, WFM | | |
| Чувствительность, мкВ (AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | FM | WFM | AM |
| | 1.6...5 МГц-0.4<br>5...30 МГц-0.25<br>30...118 МГц-0.2<br>118...175 МГц-0.18<br>175...470 МГц-0.22<br>470...1000 МГц-0.28<br>1000...1310 МГц-0.45 | 30...118 МГц-0.71<br>175...470 МГц- 0.71<br>470...1000 МГц-1.0 | 0.5...5 МГц-1.3<br>5...30 МГц-0.79<br>118...136 МГц-0.63<br>222...247 МГц -0.63<br>247...330 МГц -0.71 |
| Скорость сканирования | до 30 каналов/сек | | |
| Количество каналов памяти | 450 (400 стандартных, 50 границ сканирования) | | |
| Потребляемый ток max/min, мА | 170 / 41 | | |
| Диапазон рабочих температур | −10... +60 °C | | |
| Габариты и вес | 58×86×27 мм, 170 г | | |

## Icom IC-R20

IC-R20 является малогабаритным профессиональным широкодиапазонным сканирующим РПУ с возможностью регистрации принимаемого сигнала на встроенный цифровой магнитофон и одновременного контроля двух частот.

***Двойной прием:*** До появления ICOM IC-R20 для слежения за двумя частотами было необходимо использовать два приемника. Теперь стало возможным слежение за аварийными каналами, контроль над

воздушным движением, наблюдение за двумя водителями, прием одновременно радио- и ТВ-сигнала.

***Широкий диапазон — от КВ до СВЧ:*** ICOM IC R20 работает на частотах от 150 кГц до 3304,999 МГц в режимах SSB, CW, AM, FM, WFM с шагом перестройки от 0,01 до 100 кГц. Это позволяет принимать AM/FM-радиодиапазоны, телевизионные сигналы, радиосвязь между кораблями, самолетами, выполнять другие технические задачи.

***Цифровой диктофон на 4 часа:*** 32-мегабайтный цифровой магнитофон сканера ICOM R20 непрерывно осуществляет в течение четырех часов запись принимаемого сигнала, сохраняет принятые с эфира радиопередачи и позволяет их перезаписывать через USB-порт в ПЭВМ. Благодаря функции записи сигнала на встроенный магнитофон возможно производить запись трансляции с беспроводного (радио) микрофона в ходе переговоров. Через USB-порт можно переписать в компьютер принятую передачу или переслать по назначению. (Прослушивание на компьютере невозможно.)

***Прием сигналов с кодовым и тональным разделением каналов.*** Когда многочисленные пользователи находятся на одном канале, они используют специальную систему разделения каналов для уменьшения помех от других пользователей. Две наиболее популярные системы реализованы в ICOM R 20, это DTCS и CTCSS. По субтонам возможно сканирование

***Большая память с буквенными наименованиями каналов.*** 1000 стандартных каналов памяти, 200 автоматически сканируемых каналов и 25 пар границ сканирования. IC-R20 позволяет удобно настраиваться и записывать в память частоты сигнала с возможностью присвоения каждому каналу отдельного имени.

***До 11 часов непрерывной работы.*** Экономичность, присущая аппаратуре фирмы ICOM, реализована и в IC-R20: 11 часов работы без подзарядки от встроенного Li-Ion аккумулятора. Также ICOM R-20 может работать от трех пальчиковых батареек AA. Длительная работа, так же как и зарядка встроенного аккумулятора, возможна от прикуривателя автомобиля или входящего в комплект адаптера.

***Функции сканирования.*** IC-R20 — самый быстрый сканирующий приемник фирмы ICOM. Скорость сканирования — до 100 каналов в секунду в режиме VFO. Вы можете поместить каналы памяти внутрь динамически изменяемых банков (до 100 каналов в банке, не более 26 банков), кроме того, можно связать несколько различ-

ных банков для сканирования по банкам памяти. Дополнительно ICOM IC-R20 предлагает разнообразный контроль за сканированием, например, задержка сканирования, возобновление сканирования при определенном сигнале и т. д.

***Функция спектроанализа (Real-time bandscope):*** Спектроскоп работает в реальном времени и позволяет контролировать наличие сигналов. Иногда прослушивания сигнала недостаточно, поэтому IC-R20 имеет спектроскоп. Он используется для отображения сигнала, на частоту которого настроен приемник. Спектроскоп работает независимо от прослушивания сигнала. Дополнительная функция спектроскопа заключается в возможности определения модулированности сигналов.

| **Технические характеристики ICOM IC R20** | |
|---|---|
| частотный диапазон, МГц | 0.150 – 1304.999, 1305.0003304.999 |
| Одновременный прием двух полудуплексных частот:<br>VFO A<br>VFO B | 0.150 – 469.999МГц<br>(LSB, USB, CW, AM, FM, WFM)<br>118 – 174.999, 330 – 1304.999MHZ<br>(AM, FM, WFM) |
| Виды модуляции | LSB*, USB*, CW*, AM, FM, WFM<br>(* 0.150 – 469.999МГц) |
| Количество каналов | 1250 (1000 основных, 50 сканируемых границ и 200 автоматически записываемых) |
| Шаг перестройки частоты, кГц | 0.01, 0.1, 5, 6.25, 8.33*, 9*, 10, 12.5, 15, 20, 25, 30, 50, 100 кГц |
| Питание | 4 BP-206 или 3 батареи типа AA (56)8B (4 AA (R6)<br>Ni-Cd аккумулятора) 4,8 – 16 В<br>(источник постоянного тока) |
| Ток потребления, мА | прием: 150 (подсветка выключена)<br>режим готовности: 100 (подсветка выключена)<br>режим энергосбережения: 35 |
| Тип разъема под антенну | BNC (500 м) |
| Вес, г | 320 |
| Размеры, мм | 60×142×34,8 |
| Диапазон рабочих температур, °С | от –10 до +60 |
| Чувствительность (SSB, CW, AM — 10дБ S/N; FM, WFM — 12 дБ SmD) FM | 1.620 – 4.999 МГц — 0.56 мкВ<br>5.000 – 221.999 МГц — 0.4 мкВ<br>330.000 – 832.999 МГц — 0.56 мкВ<br>833.000 – 1304.999 МГц — 0.71 мкВ<br>1330.000 – 2304.999 МГц — 5.6 мкВ<br>2330.000 – 2999.999 МГц — 18 мкВ<br>76.000 – 108.000 МГц — 1.8 мкВ |

| | |
|---|---|
| FM | 175.000 – 221.999 МГц — 1.8 мкВ<br>470.000 – 769.999 МГц — 2.5 мкВ |
| AM | 0.495 – 4.999 МГц — 2.2 мкВ<br>5.000 – 29.999 МГц — 1.4 мкВ<br>118.000 – 135.999 МГц — 1.4 мкВ |
| SSB, SW | 0.495 – 4.999 МГц — 0.4 мкВ<br>5.000 – 29.999 МГц — 0.25 мкВ<br>50.000 – 53.999 МГц — 0.25 мкВ<br>118.000 – 146.999 МГц — 0.25 мкВ<br>330.000 – 469.999 МГц — 0.32 мкВ |
| избирательность, дБ | SSB, CW: более 1.8 кГц/-6 дБ FM,<br>AM: более 12 кГц/-6 дБ,<br>менее 30 кГц/-60 дБ<br>WFM: более 150 кГц/-6 дБ |

### Icom IC-R8500

Новейшие технологические достижения позволили фирме ICOM добиться высококачественного приема сигналов всех видов модуляции в диапазоне от коротких волн до СВЧ при постоянной чувствительности. ICOM IC-R8500 — это не просто сканер, это профессиональный связной приемник с широким набором специальных функций — начиная от скоростного сканирования и кончая развитым компьютерным интерфейсом.

Широкий диапазон: 0.1 – 2000 МГц с шагом 10 Гц.

Виды модуляции: SSB (USB, LSB), CW, AM, FM, WFM, включая специальные виды: узкая CW, широкая и узкая AM, узкая FM (для приема узкой CW требуется фильтр FL-52A).

Сверхвысокая стабильность частоты. Высокостабильный кварц (TCXO) обеспечивает стабильность менее +/-100Гц (до 30 МГц) и менее 0,3 ppt (свыше 30 МГц), что повышает качество работы схем PLL и DDS.

Повышенное качество приема. Схемы сдвига промежуточной частоты (IF shift) и режекторный аудиофильтр (APF) впервые встроены в приемник такого класса. Сдвиг ПЧ позволяет разделить близкорасположенные сигналы. Режекторный фильтр используется для подавления интерференции от наложенных друг на друга сигналов, что особенно эффективно при работе с CW. Качество приема повышается также за счет применения шумоподавителя (NB), ВЧ-аттенюатора, переключаемой АРУ и цифровой АПЧ. Чувствительность приемника в диапазоне от 2 до 1300 МГц практически не зависит от частоты.

Расширенные функции использования памяти. В каждом канале запоминается частота, вид модуляции (включая ширину полосы), шаг настройки и т. д. Для повышения эффективности память разделена на 20 банков по 40 каналов и на области автоматической записи или пропуска по 100 каналов. Каналам и банкам памяти можно присвоить буквенные имена длиной 8 и 5 символов соответственно. Дополнительно в памяти выделено 20 каналов для границ сканирования и 4 приоритетных канала. Количество каналов в каждом банке может быть изменено. Функция редактирования памяти позволяет производить копирование и вставку содержимого каналов.

Компьютерный интерфейс. На задней панели приемника расположен не только разъем CI—V, но и последовательный порт для непосредственного подключения к компьютеру. Обмен осуществляется в разработанном фирмой ICOM формате CI—V и позволяет как считывать данные (частоты, уровень сигнала), так и управлять всеми функциями приемника. Приемник ICOM IC-R8500 поддерживается большинством управляющих программ (ARCON, FILIN и др.).

7 типов сканирования: программируемое, диапазонное, по каналам памяти, по видам сигнала, по группам каналов памяти, приоритетное, с автоматической записью частот. Скорость сканирования плавно регулируется до 40 каналов в секунду (как в режиме сканирования по каналам памяти, так и при программируемом сканировании). Время задержки также плавно регулируется. Интеллектуальная система поиска голоса. VSC (Voice Scan Control) позволяет пропускать смодулированные и шумовые сигналы.

Удобство настройки. Предусмотрено два метода ввода частоты: с клавиатуры или с помощью ручки настройки. Шаг настройки регулируется в пределах от 10 Гц до 1 МГц. Дополнительно существует режим программируемого шага, устанавливаемого для каждого канала в пределах от 0,5 до 100 кГц с разрешением 0,5 кГц.

**Прочие функции:**

Автоматическое выключение (Sleep timer). 3 антенных разъема — SO-239, RCA и N-type. Стрелочный S-метр и индикатор центральной частоты. Шумоподавитель с предустановкой порогового уровня сигнала. Разъемы REC и REC-remote для записи сигналов и управления магнитофоном.

| Технические характеристики | ICOM IC-R8500 |
|---|---|
| Диапазон частот, МГц | 0.1...2000 |

| Виды модуляции | SSB (USB, LSB), AM (wide, normal, narrow), CW (normal, narrow), FM | | | | | | |
|---|---|---|---|---|---|---|---|
| Чувствительность, мкВ (SSB, CW, AM при 10 дБ S/N, FM, WFM при 12 дБ SINAD) | Диапазон, МГц | SSB, CW | AM | AM-N | AM-W | FM | WFM |
| | 0.1...0.5 | 1.0 | 6.3 | — | — | — | — |
| | 0.5...1.8 | 2.0 | 13.0 | — | — | — | — |
| | 1.8...2.0 | 0.25 | 3.2 | 3.5 | | — | — |
| | 2.0...28 | 0.2 | 2.5 | 2.0 | — | — | — |
| | 28...30 | 0.2 | 2.5 | 2.0 | — | 0.6 | — |
| | 30...1000 | 0.32 | 3.6 | 2.0 | 3.2 | 0.5 | 1.4 |
| | 1240...1300 | 0.32 | 3.6 | 2.0 | 3.2 | 0.5 | 2.0 |
| Количество каналов памяти | 1000 стандартных, 20 границ сканирования, 1 приоритетный | | | | | | |
| Потребляемый ток, А | 2.0 | | | | | | |
| Диапазон рабочих температур | −10... + 50 °C | | | | | | |
| Скорость сканирования | 10 — 40 каналов в секунду (при сканировании из памяти и программируемом канале) | | | | | | |
| Габариты и вес | 287 × 112 × 309 мм, 7.0 кг | | | | | | |

## 5.2. Технические средства защиты информации

### 5.2.1. Подавители диктофонов

#### Подавитель диктофонов «Барсетка»

**Назначение**

Предназначен для предотвращения утечки информации за счет несанкционированного (скрытного) применения диктофонов и других портативных средств звукозаписи в оперативных условиях.

**Особенности**

Позволяет бороться с любыми типами диктофонов (цифровые и кинематические).

Подавитель выполнен в виде барсетки со встроенной антенной. Лепесток излучения в этом случае направлен перпендикулярно боковой поверхности барсетки.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Дальность подавления цифровых диктофонов | до 1 метра |
| Дальность подавления кинематических диктофонов | до 1,5 метров |
| Время непрерывной работы | 30 мин |
| Управление | радиоканал |
| Антенна | встроенная |

## Подавитель диктофонов и сотовых телефонов в кейсе «Сапфир-КМ»

**Назначение**

Предназначен для предотвращения утечки информации за счет несанкционированного (скрытного) применения диктофонов и сотовых телефонов.

Подавитель выполнен в виде кейса со встроенной антенной. Лепесток излучения в этом случае направлен перпендикулярно поверхности кейса.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| **Подавитель диктофонов** | |
| Дальность подавления цифровых диктофонов | до 2 метров |
| Дальность подавления кинематических диктофонов | до 3,5 метров |
| Время непрерывной работы | 1,5 часа |
| Управление | радиоканал, ручное |
| Антенны | встроенные |
| **Подавитель сотовых телефонов** | |
| Подавляемые стандарты | GSM, CDMA, DAMPS, AMPS (дополнительно NMT) |
| Выходная мощность | 8 Вт |
| Типовая дальность подавления | до 30 м |
| Антенны | встроенные |
| Возможность регулировки | отсутствует |
| Управление | радиоканал |
| Время непрерывной работы | 1 час |

## Стационарный 2-канальный подавитель диктофонов «Сапфир-2»

**Назначение**

Предназначен для предотвращения утечки информации за счет несанкционированного (скрытного) применения диктофонов и других портативных средств звукозаписи в стационарных условиях.

**Особенности**

В отличие от одноканального подавителя «Сапфир» имеет два канала мощности и, следовательно, в два раза большую мощность.

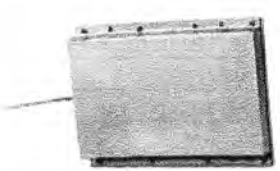
Позволяет бороться с любыми типами диктофонов (цифровые и кинематические). Дальность подавления лежит в следующих пределах: цифровые диктофоны: до 3 метров; кинематические диктофоны: до 5 метров.

Подавитель состоит из генератора сигнала помехи и внешней направленной излучающей антенны. С одним генератором одновременно применяются две антенны.

Возможные типы применяемых антенн:

- Антенна с излучением в противоположные стороны — предназначена для различных условий применения, как для защиты столов, так и в портативных условиях. Имеет один лепесток излучения, направленный перпендикулярно плоскости антенны. Лепесток имеет размеры: 60 × 80° (в горизонтальной и вертикальной плоскостях соответственно).
- Антенна с излучением перпендикулярно плоскости — предназначена для различных условий применения, как для защиты столов, так и в портативных условиях. Имеет один лепесток излучения, направленный перпендикулярно плоскости антенны. Лепесток имеет размеры: 60 × 80° (в горизонтальной и вертикальной плоскостях соответственно).

*Антенна с излучением в противоположные стороны*



*Антенна с излучением перпендикулярно плоскости*

Система устанавливается стационарно под поверхностью стола переговоров.

В зависимости от конкретных условий проведения переговоров,

выбираются антенны с требуемой диаграммой направленности. С одним генератором могут применяться антенны разных типов, это позволяет сформировать практически любую нужную зону подавления.

## 5.2.2. Акустические рефлектометры

### Акустический рефлектометр «Арфа-М»

**Назначение**

Акустический рефлектометр «Арфа» — это индикаторный прибор для проверки радиоэлектронной аппаратуры, подключаемой к проводным силовым и коммуникационным линиям, и поиска линейных закладок параметрического типа методом высокочастотного зондирования (при этом такие закладки формируют сигнал с фазовой угловой или амплитудной модуляцией, который и выявляется «Арфой» в диапазоне от 50 кГц до 30 мГц).

**Особенности**

Изделие «Арфа» первоначально разрабатывалось для проверки аппаратуры, используемой в режимных помещениях. Однако его возможности позволяют использовать его при подключении напрямую к различным питающим и телефонным сетям. Вместе с тем качественное исследование таких сетей может потребовать использования дополнительных фильтровых схем, снижающих уровень помех (поставляются дополнительно).

Модель «Арфа-М» в отличие от модели «Арфа» обеспечивает возможность работы в режиме «Автоматического поиска» и позволяет автоматически оценить качество сигнала в линии в диапазоне заданных частот при параметрах сигнала возбуждения, установленных в режиме ручного поиска.

В настоящее время завершается разработка новой модели — «Арфа-200М», работающей в расширенном до 200 ГГц диапазоне частот.

**Принцип действия:**

Принцип действия изделия основан на селекции и амплитудно-фазовой демодуляции сигнала в линии. Чувствительность приема и уровень сигнала возбуждения определяются коэффициентом

усиления соответствующих регулируемых усилителей. Блок управления формирует сигналы для настройки синтезаторов частот и обеспечивает интерфейс взаимодействия с оператором. Алгоритм исследования сводится к подбору оптимальных соотношений параметров настройки для получения сигнала отклика наилучшего качества.

С помощью активной аудиоколонки можно провести поиск отклика по методу акустозавязки. При этом сигнал с выхода изделия подается на аудиоколонки, установленные вблизи от исследуемого объекта.

Ручной режим обеспечивает возможность прослушивания диапазона на заданной частоте с выбранными параметрами, запись результата в протокол измерений, сохранение протокола в архивном файле и последующую загрузку этого файла для работы. Кроме того, в ручном режиме возможно автоматическое сканирование в допустимом диапазоне частот с фиксированным временем прослушивания.

В режиме автопоиска обеспечивается автоматический поиск в установленном диапазоне частот по заданному порогу обнаружения и запись результатов в протокол измерений. При превышении порога обнаружения поиск может быть остановлен, а оператор имеет возможность прослушать выбранную частоту, изменяя параметры, сохранить или удалить ее в протоколе измерений и продолжить поиск в указанном диапазоне частот. Результатом работы является протокол исследования, где ведется регистрация параметров возбуждения линии, при которых был установлен факт наличия канала утечки информации.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Время автономной работы при полностью заряженном аккумуляторе | не менее 4 часов |
| Диапазон частот навязывания | 50 кГц — 30 мГц |
| Шаг перестройки по частоте сигнала навязывания | 1 кГц |
| Минимальный уровень обнаружения сигнала отклика в линии сопротивлением 200 Ом | не менее 100 дБ |
| Напряжение сигнала возбуждения в линии сопротивлением 200 Ом | не менее 1,0 В |

### 5.2.3. Средства защиты по виброакустическому каналу

#### Адаптивный генератор виброакустической помехи «Кедр»

**Назначение**

Адаптивный генератор виброакустической помехи «Кедр» предназначен для защиты выделенных помещений от утечки акустиче-

ской информации по вибрационному и акустическому каналам. Его принцип действия основан на маскировании речи шумовой помехой, которая создается с помощью виброизлучателей. Противодействие прослушиванию заключается в излучении шумовой помехи в элементы строительных конструкций здания. Прибор предотвращает возможность прослушивания переговоров с помощью акустических, вибрационных датчиков, лазерных устройств съема информации, аппаратуры прослушивания через стены, потолки, перекрытия, окна, воздуховоды, трубы отопления и т. п.

**Особенности**

Устройство реализует распределенную виброакустическую защиту помещения через сеть излучателей малой мощности, что позволяет надежно закрыть локальные области утечки информации по виброакустическому каналу (микротрещины, полости и т. п.), а также снизить общий уровень акустического фона в защищаемом помещении.

Прибор может работать в двух режимах: «1» — адаптивный, «2» — непрерывный. При работе в режиме «1» обеспечивается оптимальное перекрытие уровня речи уровнем помехи в строительных конструкциях, а также минимальное излучение шума в само помещение. В режиме «2» прибор работает в непрерывном режиме. К устройству могут подключаться до 20 излучателей типа «ПКИ-1» (для зашумления строительных конструкций), по 10 излучателей на каждый канал, а также до 4 электромагнитных излучателя типа «ЭМ-1» для зашумления воздуховодов. Все три канала подключения имеют независимую регулировку, что позволяет выставлять необходимый для защиты уровень шума на стенах, на окнах, трубах отопления.

В каждом канале генератора имеется цифровой 5-полосный графический эквалайзер, позволяющий проводить настройку канала под конкретные условия (стена, окно и т. п.) и различные виды вибродатчиков. Наличие встроенный памяти позволяет запоминать до 16 вариантов амплитудно-частотных характеристик эквалайзера (по 4 на каждый канал). Система акустопуска и наличие ДУ (проводного или по радиоканалу) дает возможность осуществлять гибкое управление процессом генерации помехи.

В устройстве имеется встроенная система контроля состояния каналов, позволяющая определить как перегрузку любого из них, так и отсутствие подключенных датчиков.

Система акустической и виброакустической защиты «КЕДР» прошла сертификационные испытания по требованиям Гостехкомиссии РФ (Сертификат № 722) и Минобороны РФ (Сертификат № 150) и может использоваться в выделенных помещениях до 1-й категории включительно. Изделие «Кедр» защищено патентом РФ на полезную модель № 30478.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Полоса частот сигнала защиты | 200 Гц – 15 кГц |
| Количество каналов | 3 |
| Максимальное количество виброизлучателей, подключаемых на 1-й и 2-й канал | 20 |
| Максимальное количество акустоизлучателей | 4 |
| Радиус действия одного вибродатчика | 1,5 м |
| Количество подключаемых микрофонов | 2 |
| Минимальное сопротивление акустоизлучателей | 4 Ом |
| Потребляемая мощность, не более | 20 ВА |
| Габаритные размеры | 160 × 220 × 54 |

## Система виброакустического зашумления «Шорох-2»

**Назначение**

Система виброакустического зашумления «Шорох-2» предназначена для защиты выделенных помещений по виброакустическому каналу.


**Особенности**

Высокий КПД и низкий уровень паразитного акустического зашумления. Пятиполосный эквалайзер позволяет оптимальным образом сформировать спектр сигнала помехи и выполнить требования по защите помещения при обеспечении максимальной комфортности переговоров. Более высокий радиус действия вибропреобразователей позволяет выполнить требования по защите помещений, применяя меньшее количество преобразователей.

**Базовый комплект поставки:**

Генератор сигнала помехи ГШВА-1.

Вибропреобразователь на стену КВП-2.

Вибропреобразователь на стену КВП-6.
Вибропреобразователь на стену КВП-8.
Вибропреобразователь на оконное стекло КВП-7.
Вибропреобразователь скрытой установки в стену КВП-10.
OMS-2000 акустический излучатель.

**Технические характеристики**

| **Наименование**<br>Вид сигнала помехи | **Значение**<br>аналоговый шум с нормальным распределением плотности вероятности мгновенных значений |
|---|---|
| Диапазон генерируемых частот | 175 – 5600 Гц |
| Пятиполосный октавный эквалайзер с глубиной регулировки по полосам | ±20 дБ |
| Глубина регулировки уровня сигнала помехи | не менее 40 дБ |
| Регулировка уровней акустической и виброакустической помехи | раздельная |
| Применяемые типы вибропреобразователей | КВП-2, КВП-6, КВП-8 (стеновые) и КВП-7 (оконный) |
| Эффективный радиус действия КВП-2, КВП-6, КВП-8 на перекрытии толщиной 0,25 м | 6 ±1 м |
| Эффективный радиус действия КВП-7 на стекле толщиной 4 мм | 1,5 ±0,5 м |
| К генератору одновременно могут подключаться | вибропреобразователи КВП-2 – 24 шт., КВП-7 – 16 шт. и акустические колонки (8 Ом) — 16 шт. |
| Максимальная суммарная выходная мощность | 19 Вт |
| Габариты блока генератора | 280 × 270 × 120 мм |
| Вес генератора | не более 6 кг< |
| Габариты и масса вибропреобразователей | КВП-2: 0 40 × 30 мм; вес: 250 г; КВП-6: 0 50 × 39 мм; вес: 550 г; КВП-7: 0 30 × 10 мм; вес: 20 г; КВП- 8: 0 40 × 36 мм; вес: 300 г |

## 5.2.4. Средства криптографической защиты

### Криптомаршрутизатор «Citadel VPN»

**Назначение**

Криптомаршрутизатор Citadel™ VPN предназначен для организации

защищенных корпоративных сетей (Virtual Private Network) на базе сетей общего пользования с протоколом TCP/IP (Internet).

Криптомаршрутизатор обеспечивает конфиденциальность и защиту от искажений информации, передаваемой друг другу защищенными подсетями корпоративной сети через транспортную сеть общего пользования, а также сокрытие структуры корпоративной сети и защиту ее узлов от атак извне.

Криптомаршрутизатор может использоваться как в паре с межсетевым экраном Citadel™ Firewall, так и отдельно.

**Особенности**

В комплекте с устройством поставляется программное средство Citadel™ VPN ControlCenter, которое выполняет выработку конфигурационной информации и генерацию ключей для каждого устройства Citadel™ VPN в корпоративной сети и подготовку смарт-карт для каждого устройства.

**Базовый комплект поставки:**

Статическая маршрутизация TCP/IP.

Шифрование IP-трафика, передаваемого через сеть общего пользования, в соответствии с ГОСТ 28147-89. Используется защищенный инкапсуляционный протокол собственной разработки. Для каждого защищенного маршрута устанавливается отдельный ключ парной связи.

Возможность применения платы аппаратного шифрования ISA или PCI.

Защита от искажения IP-пакетов, передаваемых через сеть общего пользования, обеспечивается вычислением имитоприставки на каждый пакет в соответствии с ГОСТ 28147-89.

Маскирование структуры подсетей, составляющих корпоративную сеть.

Защита внутренних подсетей и их ресурсов от внешних атак.

Защита от внутренних атак типа «IP-spoofing».

Защита самого устройства от внешних и внутренних атак типа «отказ в обслуживании», например атак «ping-flooding».

Защита от ранее переданной информации.

Защита от передачи открытой информации во внешний интерфейс. Удаленный мониторинг с использованием защищенного протокола мониторинга.

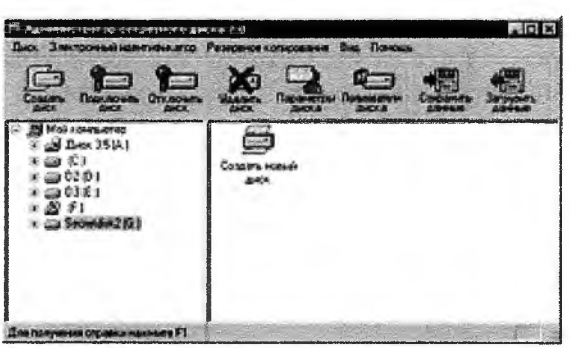
Ведение протокола работы и передача протокола во внутреннюю сеть с помощью syslog.

**Технические характеристики**

| **Наименование** Процессор | **Значение** Intel Pentium 166/200 MHz |
|---|---|
| Внутренняя шина | PCI |
| Оперативная память (RAM) | 16 MB, расширяемая до 64MB |
| ROM | 0.5 MB, расширяемая до 8 MB |
| Flash память | 0.5 MB, расширяемая до 4 MB |
| Устройство ввода конфигурации | Считыватель смарт-карт (I2C) |
| Сетевые интерфейсы | в базовой конфигурации 2 порта IEEE 802.3 10Base-T/100Base-TX UTP, Full or Half Duplex (занят один слот PCI) |
| **Программный криптографический модуль** | |
| Скорость шифрования «память — память» | Более 1.7 Мб/сек при использовании процессора Intel Pentium 166 |
| ИК-защита | Применяется ряд методов |
| Выработка сеансовых ключей и синхропосылок | Высоконадежный программный датчик случайных чисел или аппаратный ДСЧ на специальной плате |
| **Физические параметры** | |
| Суммарная пропускная способность | 500 Кб/сек при работе на канале Ethernet 10 Мб/сек и использовании программной реализации шифрования |
| Пропускная способность маршрутизатора | 7000 пакетов в секунду |
| Габаритные размеры | 18×43×46 см |
| Вес | 6 кг |
| Наработка на отказ (MTBF) | >40,000 час |

## Системы криптографической защиты информации «Secret Disk»

**Назначение**



Системы защиты информации семейства «Secret Disk» позволяют защищать информацию путем организации для конкретных пользователей ПЭВМ защищенных носителей информации — виртуальных логических дисков. Вся информация, записываемая на такие носители, подвергается «прозрачному» (на лету) преобразованию с использованием одного из следующих алгоритмов:

- встроенный алгоритм преобразования данных с длиной ключа 128 бит;
- входящая в Windows реализация RC-4 (с длиной ключа 40 бит);
- алгоритм шифрования по ГОСТ 28147—89 с длиной ключа 256 бит (при использовании эмулятора платы «Криптон», имеющего сертификат ФАПСИ).

**Особенности**

- организация многопользовательского доступа к одному защищаемому носителю информации;
- формирование защищенных архивов для передачи по открытым каналам связи;
- блокировка доступа к защищаемой информации при подаче сигнала тревоги либо при входе в систему в режиме «работа под принуждением»;
- блокировка ПЭВМ при изъятии аппаратного носителя ключевой информации.

Семейство средств защиты информации «Secret Disk» включает в себя модификации для защиты информации на автономных ПЭВМ и комплексы защиты информации, хранимой и обрабатываемой на выделенных серверах ЛВС.

**Принцип работы:**

Для активизации доступа к защищенному носителю (диску) информации пользователю необходимо подключить аппаратный идентификатор и осуществить ввод ключевой информации. В качестве аппаратных идентификаторов могут использоваться:

- электронные USB-брелки;
- PCMCIA-карты;
- электронные ключи для сот-порта;
- смарт-карта.

До момента активизации защищаемый носитель (диск) представляет собой файл на жестком диске ПЭВМ.

## 5.2.5. Устройства защиты от утечки акустической информации

### Акустический генератор шума «WNG-023»

**Назначение**

Акустический генератор шума WNG-023 предназначен для защиты переговоров от любых видов съема акустической информации.

**Особенности**

Принцип действия основан на постановке акустической помехи речевого диапазона частот. Перед началом проведения переговоров генератор устанавливается в защищаемом помещении максимально близко к наиболее вероятному месту размещения устройств съема акустической информации (например, дверь).

Максимальный защищаемый объем составляет 50 м$^3$.

### Акустический маскиратор конфиденциальных переговоров «Букет»

**Назначение**

Устройство защиты речевой информации «Букет» предназначено для маскирования речи двух или более собеседников методом акустического зашумления помещения, в котором ведутся переговоры.

**Особенности**

«Букет» состоит из двух функциональных частей: блока обработки, располагающегося в чемодане, и микрофона. Блок обработки представляет собой автономный модуль с возможностью работы как от сети переменного тока, так и от встроенных аккумуляторов, размещенный в стандартном кейсе. Основу платы блока составляет быстродействующий микропроцессор фирмы «Texas Instruments».

В отличие от существующих аналогичных устройств «Букет» обеспечивает наибольший комфорт при ведении разговора при аналогичной или более высокой степени защищенности информации, т. к. постоянно отслеживается спектральный состав речи собеседни-

ков и ее громкость, и зашумление происходит в этой же полосе и с пропорциональной интенсивностью.

**Принцип работы**

В зоне разговора, чаще всего ограниченной площадью стола, располагается микрофон. В двух – пяти метрах ставится блок обработки со встроенными громкоговорителями. При попадании в него речевого сигнала определяется мощность каждой его спектральной составляющей. Затем блок вырабатывает сигнал зашумления, поступающий в громкоговорители, спектральный состав и мощность которого соответствуют спектральному составу и мощности речи собеседников. В паузах разговора зашумление отсутствует.

Таким образом, «Букет» обеспечивает маскирование речи от всех известных устройств прослушивания, поскольку за границами «зоны защиты» присутствует смесь речевого сигнала и шумового, причем шумовая составляющая значительно превосходит речевую.

По оценке экспертов, в условиях появления все более совершенных и не выявляемых существующими приборами устройств негласного съема и записи информации (сотовые телефоны, цифровые диктофоны и др.) акустический маскиратор зачастую остается единственным средством, обеспечивающим гарантированное закрытие всех каналов утечки речевой информации. Особенно актуальным является его использование для обеспечения конфиденциальности переговоров в нестандартной обстановке (автомашина, чужой офис, ресторан и т. п.).

**Технические характеристики**

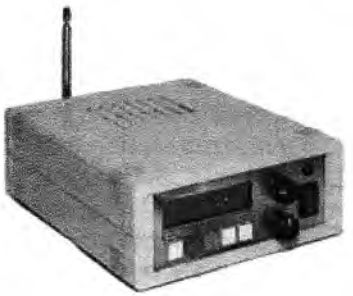
| Наименование | Значение |
|---|---|
| Устройство питается от сети переменного тока | 220В/ 50 Гц |
| Максимальная потребляемая мощность (в режиме зарядки) | 10 Вт |
| Время работы устройства в автономном режиме (при полной зарядке аккумулятора) | не более 60 мин |
| Масса прибора | не более 4 кг |

## Скоростной автоматический поисковый приемник ближней зоны с генератором прицельной помехи «Октава-СК»

**Назначение**

Скоростной поисковый приемник радиосигналов «ОКТАВА-СК» является стационарным средством радиотехнического контроля, предназначенным для быстрого (не более 15 секунд) автоматического обнаружения сигналов, излучаемых нелегальными радиопередат-

чиками, и подавления каналов их приема (совместно с усилителем мощности «ОКТАВА-УМ»).



**Особенности**

Изделие «Октава-СК» позволяет:

- производить изучение радиоэлектронной обстановки в конкретном месте его эксплуатации с запоминанием частот сигналов;
- обнаруживать и определять местоположение нелегально существующего передатчика в контролируемом помещении;
- подавлять канал приема сигнала обнаруженного нелегального передатчика путем постановки на его частоте прицельной помехи;
- проверять работоспособность приемников, индикаторов поля, частотомеров и других технических средств с помощью встроенного тестового генератора.

**Базовый комплект поставки:**

Изделие «Октава-СК».
Антенна.
Техническое описание и инструкция по эксплуатации.
Упаковка.
ВЧ-кабель.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Диапазон принимаемых частот | 30 – 2000 МГц |
| Чувствительность, мкВ | в диапазоне 30 – 1000 МГц: не более 25<br>в диапазоне 1000 – 2000 МГц: не более 1000 |
| Полоса пропускания на промежуточной частоте | 200 Гц |
| Время просмотра диапазона, не более | 15 сек, при отсутствии сигнала 10 сек |
| Точность измерения частоты | 10 кГц |
| Диапазон измерения уровня входного сигнала | 50 дБ, с включением аттенюатора: 70 дБ |
| Количество исключаемых каналов приема | 4850 |
| Количество запоминаемых обнаруженных сигналов | 256 |

## 5.2.6. Устройства защиты от утечки информации по каналам ПЭМИН

### Генератор шума «Гном-3»

**Назначение**

Генератор шума «Гном-3» предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации.

Генератор имеет внешнюю гибкую рамочную антенну (в комплект поставки не входит), которая устанавливается стационарно в защищаемом помещении. Антенна представляет собой три рамки размером 3 × 5 метров, расположенные во взаимно перпендикулярных плоскостях. В основном данный генератор используется для защиты залов вычислительной техники общей площадью до 50 м.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Диапазон рабочих частот | 0,1 – 1000 МГц |
| Спектральная плотность шума | 45 – 75 дБ |
| Индикация работы | световая |

### Генератор шума «ГШ-2500»

**Назначение**

Генератор шума «ГШ-2500М» предназначен для защиты информации от утечки, обусловленной побочными электромагнитными излучениями и наводками ПЭВМ и других средств обработки информации.

**Особенности**

Генератор имеет внешнюю жесткую рамочную антенну диаметром 60 см.

Может применяться для защиты не более одного автоматизированного рабочего места.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Диапазон рабочих частот | 0,1 – 2500 МГц |
| Спектральная плотность шума | 45 – 75 дБ |
| Индикация работы | световая, звуковая |

## 5.2.7. Блокираторы сотовых телефонов

### Блокиратор каналов сотовой связи «Октава-2С»

**Назначение**

Изделие «Октава-2С» предназначено для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи стандартов GSM-900/1800, E-GSM, AMPS/DAMPS, CDMA, и блокирования работы телефонов названных систем мобильной связи в пределах выделенных помещений, предназначенных для ведения переговоров, проведения совещаний. Используется в целях предотвращения утечки информации за пределы выделенного помещения через подслушивающие устройства указанного выше типа, через включенный телефон мобильной связи, а также для обеспечения рабочей обстановки во время проведения переговоров, совещаний.

**Принцип действия**

В зависимости от расстояния до ближайшей базовой станции, зона эффективного действия прибора составляет от 3 м до 15 м. Телескопические антенны должны быть установлены в вертикальное положение и выдвинуты на все секции.

Изделие излучает в диапазоне работы систем мобильной связи, мощность излучения в других диапазонах незначительна. Изделие имеет небольшую мощность излучения (меньше мощности мобильных телефонов), блокирование каналов систем мобильной связи осуществляется за счет применения специального вида модуляции. Изделие не оказывает влияния на работу других технических средств — бытовой электронной техники (теле-, видео-, аудио- и др.), компьютеров, оргтехники. Для охвата большей площади необходимо использовать несколько изделий, разнесенных по защищаемой территории.

### Технические характеристики

| Наименование | Значение |
|---|---|
| Диапазон рабочих частот GSM | 860/960,1800/1900 МГц |
| Мощность излучения | не более 400 мВт на диапазон |
| Максимальная зона блокирования | от 3 до 15 м (зависит от расстояния до ближайшей базовой станции) |
| Напряжение питания | переменное напряжение 220В/50Гц |
| Потребляемая мощность | не более 10 ВА |
| Габаритные размеры | 200 × 150 × 60 мм |
| Вес изделия | не более 2 кг |

## Миниатюрный подавитель сотовых телефонов «Мозаика-мини»

**Назначение**

Предназначен для предотвращения утечки информации за счет несанкционированного использования сотовых телефонов. Также может применяться в помещениях, где использование сотовых телефонов нежелательно (театры, залы переговоров и т. п.). Принцип подавления основан на постановке узкополосной помехи приемному каналу телефона.

Устройство выполнено в виде миниатюрного радиовещательного FM-приемника, что позволяет применять его скрытно.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Подавляемые стандарты | GSM, CDMA, DAMPS, AMPS |
| Выходная мощность | 0,1 Вт |
| Типовая дальность подавления | 2 м |
| Антенна | встроенная |
| Возможность регулировки дальности подавления | отсутствует |
| Время непрерывной работы | 40 мин |
| Питание | две батареи AA |

## Подавитель сотовых телефонов в настольных часах «Мозаика-НЧ»

**Назначение**

Предназначен для предотвращения утечки информации за счет несанкционированного использования сотовых телефонов. Также

может применяться в помещениях, где использование сотовых телефонов нежелательно (театры, залы переговоров и т. п.). Принцип подавления основан на постановке узкополосной помехи приемному каналу телефона.

**Изделие закамуфлировано в настольных электронных часах.**

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Подавляемые стандарты | GSM, CDMA, DAMPS, AMPS |
| Выходная мощность | 0,5 Вт |
| Типовая дальность подавления | 3 – 15 м |
| Антенны | внешняя, скрытая (подставка под ручку) |
| Возможность регулировки | отсутствует |
| Время непрерывной работы | 24 часа |
| Питание | 220 В |

## 5.2.8. Устройства защиты от утечки информации в инфракрасном диапазоне

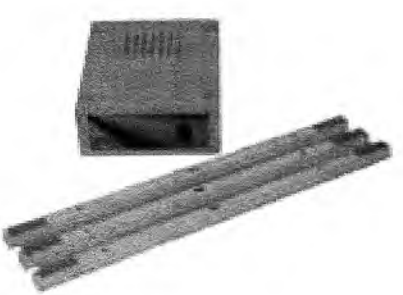
### Генератор шумовой помехи в ИК-диапазоне «Октава-ИК»

**Назначение**

Устройство «Октава-ИК» предназначено для блокирования потенциальных каналов утечки информации в ИК-диапазоне с помощью создания шумоподобной поднесущей волны, модулирующей источники излучений в ближнем ИК-диапазоне 0,85 – 0,9 мкм.

**Особенности**

«Октава-ИК» представляет собой четырехканальное устройство, конструктивно выполненное в виде блока в пластмассовом корпусе и восьми выносных излучателей, по два излучателя на один канал, которые размещаются в оконных проемах. Излучатели соединяются с блоком шлейфом проводов.



Выносные инфракрасные излучатели для генератора шума в ИК-диапазоне «Октава-ИК» представляют собой узкие пластмассовые коробки с вмонтированными в них ИК-излучателями. Крепеж каждой коробки к оконному стеклу осуществляется при помощи прилагаемых в комплекте самоклеящихся площадок (по 3 площадки на один излучатель).

В стандартную комплектацию генератора «Октава-ИК» входит 4 излучателя. Площадь покрытия одним излучателем составляет примерно 600 – 1500 мм (ориентировочно два излучателя на каждое защищаемое окно).

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Полоса частот помехи, МГц | 2 |
| Максимальный угол излучения, град | 80 |
| Мощность излучения одного канала | 1,3 Вт |
| Угол излучения | ±10 град |
| Максимальное количество излучателей в рамке | 16 |
| Плотность излучения 1-го излучателя, мВт/стер | 40 |
| Потребление электронного блока, не более, Вт | 20 |
| Питание изделия от сети переменного тока | 220 В/50 Гц |

## 5.2.9. Криминалистические средства защиты

### Комплект идентификационных средств серии Люмограф 3-БК

**Назначение**

Для нанесения на документы, предметы, поверхности и другие объекты скрытного (невидимого и не люминесцирующего в УФ-лучах) слоя идентификационного порошка, обеспечивающего возможность установления факта контакта рук или предметов с обработанной поверхностью и выявления следов их последующих контактов. Выявление осуществляется визуально, по возникающему свечению в УФ-лучах (365 нм) после обработки частиц идентификационного порошка проявляющим составом.

Нанесение скрытного слоя идентификационного порошка и проявляющего состава производится из аэрозольного баллона. Следы обработки могут быть удалены с поверхности при помощи тампона, пропитанного смывкой.

**Комплект поставки**

- Проявитель (аэрозоль) — 2 шт.
- Пыль (аэрозоль) — 1 шт.
- Смывка (аэрозоль) — 1 шт.
- Штемпельная краска (пузырек) 20 мл — 1 шт.
- Порошок (пузырек) — 1 шт.
- Штамп с набором шрифтов — 2 шт.
- Цифры мал. — 1 шт.
- Цифры бол. — 1 шт.
- Пробоотборник — 5 уп.
- Перчатки — 1 пара
- Пинцет — 1 шт.
- Ручка — 1 шт.
- Пенал:
- Фломастер — 2 шт.
- Запаска — 1 шт.
- Карандаш — 1 шт.
- Ластик — 1 шт.
- Блокнот — 1 шт.
- УФ-осветитель — 1 шт.
- Аккумуляторы — 4 шт.
- ЗУ — 1 шт.
- Упаковка-укладка (кейс) — 1 шт.
- Упаковка-вкладыш для размещения принадлежностей — 1 шт.

**Технические характеристики**

| Наименование | Значение |
|---|---|
| Длина волны ультрафиолетового излучения, вызывающего люминесценцию следа метящего препарата | 365 нм |
| Габаритные размеры изделия (кейса) | не более 410 × 300 × 90 мм |
| Масса изделия | не более 4,0 кг |
| Диапазон рабочих температур | от 0° до + 40 °С |

### Портативный ультрафиолетовый осветитель Гриф-2м

Представленный перечень технических средств отнюдь не исчерпывающий. Сегодня на рынке безопасности представлено огромное количество компаний, производящих различные технические средства. Какое в итоге выберете вы, зависит, естественно, от ваших возможностей и задач.

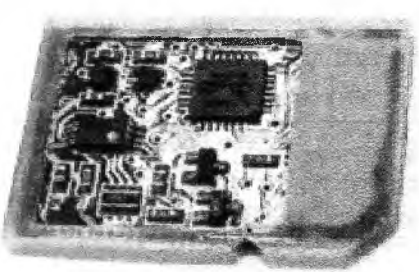
## 5.2.10. Устройства защиты от прослушивания каналов сотовой связи

### Программно-аппаратный комплект для защиты переговоров в сетях GSM – «Референт-ПДА»

Программно-аппаратный продукт «Референт-ПДА» разработан для устройств типа смартфон (коммуникатор), работающих под управлением операционной системы Windows Mobile 2003/2005. «Референт ПДА» позволяет предотвратить прослушивание переговоров, ведущихся между двумя коммуникаторами. Комплект состоит из SD/miniSD/microSD-модуля, программного обеспечения и смартфона qtek-8500.

**Запуск программы**

осуществляется автоматически при подключении SD/miniSD/microSD-модуля «Референт-ПДА», при этом на экране коммуникатора в правом нижнем углу появляется значок индикации запуска программы в фоновый режим.



Для вызова другого абонента в защищенном режиме необходимо нажать на значок индикации и далее произвести в открывшейся программе «Референт-ПДА» те же действия, что и при обычном вызове. При поступлении звонка от другого комплекта «Референт-ПДА» вместо программы

«телефон» автоматически открывается интерфейс программы «Референт-ПДА», далее все действия, как при обычном звонке.

**Интерфейс программы**

содержит: наборное поле, кнопки управления вызовом, кнопку отмены ввода последней цифры и индикатор, который отображает набираемый номер, номер вызывающего абонента при входящем вызове, состояния при установлении соединения и т. п.

Внизу диалогового окна расположено меню «Tools». Путем выбора различных пунктов меню возможно: произвести настройку уровней громкости, произвести ввод ключевой информации, произвести выход из программы.

В процессе установления соединения производится обмен специальной информацией для взаимной аутентификации устройств и формирования сеансового ключа. Данный обмен сопровождается статусной надписью «Key exchange». По окончании обмена выводится надпись «Call established xxxx», где xxxx — шестнадцатизначное число, являющееся результатом вычисления хэш-функции над сеансовой ключевой информацией. Число xxxx должно быть одинаковым у обоих абонентов. Абоненты должны убедиться в этом путем сообщения голосом противоположному абоненту своего числа. Если числа получились разными, в целях безопасности необходимо прервать текущий сеанс связи и установить соединение заново.

Прием и осуществление незащищенного голосового вызова производится с помощью стандартного программного обеспечения коммуникатора.

В случае несовпадения ключей у абонентов сеанс связи не установится и выдается сообщение «Keys arent match!».

Основным отличием изделия от аналогов является использование низкоскоростного канала передачи данных (до 1600 бод), что позволяет работать при слабом GSM-сигнале (в местах плохого приема), в роуминге, при использовании различных операторов и т. п.

Коммуникаторы, с которыми комплект проверен на совместимость:

Qtek S110; Qtek 8500(microSD); Qtek S200; Qtek 2020i; Qtek 8310 (miniSD);

I-mate JAM; I-mate JAMIN; I-mate PDA 2K.

Коммуникаторы, с которыми данный комплект не работает: Asus p505.

Остальные коммуникаторы рекомендуется проверить на совместимость перед приобретением.

**Технические характеристики модели:**

| Операционная система | Windows mobile 2003/2005 |
|---|---|
| Требуемые слоты | SD/miniSD |
| Время синхронизации: по протоколу V.110/V.32, не менее | 5 сек/20 сек |
| Скорость передачи данных, не менее | 1600 бод |

## Устройство для защиты от прослушивания сотового телефона в режиме негласной активации – SPYCASE-1.5

SPYCASE-1.5 (СПАЙКЕЙС, версия 1.5) предназначен для защиты речевой информации в случае негласной активации дистанционного прослушивания сотового телефона. При негласной активации сотовый телефон не подает никаких сигналов, но включает микрофон в режим повышенной чувствительности и начинает передавать все разговоры, ведущиеся вокруг.

SPYCASE представляет собой чехол для сотового телефона со встроенным электронным модулем. Принцип действия SPYCASE основан на постоянном мониторинге излучения вашего сотового телефона. Если ваш сотовый телефон, находясь в чехле, начал передавать речевую информацию, SPYCASE включает звуковую помеху (шум), гарантированно заглушающую любой разговор, ведущийся рядом с телефоном.

SPYCASE отслеживает все частоты стандартов GSM, CDMA-2000, UMTS, а также Bluetooth и WLAN (2,4ГГц). В случае передачи информации по этим каналам SPYCASE включает звуковую помеху.

Для обработки сигналов GSM SPYCASE использует специальный алгоритм распознавания посылок, несущих звуковую информацию. Таким образом, уменьшается количество ложных срабатываний на различные служебные сигналы (регистрация в соте, СМС и прочие).

В SPYCASE отсутствует механический выключатель питания, что положительно сказывается на надежности работы устройства.

### Внешний вид и варианты изготовления

На боковой панели чехла расположены светодиод (LED) и кнопка включения (BUTTON). Сотовый телефон должен располагаться в чехле

так, чтобы микрофон сотового телефона был рядом с динамиком (SPEAKER).

На фотографиях изображен только один из вариантов изготовления SPYCASE на основе чехла класса «Стандарт».

Возможно изготовление SPYCASE с использованием других типов чехлов. Возможно изготовление SPYCASE без светодиода. Возможен вариант настольного применения SPYCASE.

**Режимы работы и индикация**

В режиме контроля радиоэфира светодиод коротко мигает приблизительно раз в 2,5 секунды. С той же частотой происходит контроль радиоэфира. Короткое нажатие кнопки в этом режиме подтверждается коротким звуковым сигналом.

Если SPYCASE обнаруживает передачу речевой информации, он переходит в режим звуковой помехи. Включается генератор шума, светодиод начинает часто мигать. При прекращении передачи информации SPYCASE вновь переходит в режим контроля радиоэфира.

В спящем режиме светодиод не мигает, на короткое нажатие кнопки SPYCASE не реагирует. Потребление в спящем режиме крайне мало, что позволяет не извлекать элемент питания, даже если вы делаете длительный перерыв в использовании SPYCASE.

**Технические характеристики модели**

| | |
|---|---|
| Напряжение питания, в мин/макс | 2,0/3,3 |
| Потребление в спящем режиме, мкрА тип/макс | 2,4/4,0 |
| Потребление в режиме контроля, мкрА тип/макс | 100/120 |
| Потребление в режиме помехи, мАтип/макс | 9/13 |
| Частотный диапазон, МГц | 300–3000 |
| Температурный диапазон, гр. С | от –20 до +50 |
| Время работы в режиме контроля CR2032, дней | 90 |
| Время работы в режиме контроля CR1632, дней | 50 |

## Мобильный телефон для защиты переговоров в сетях GSM – TopSec GSM

Мобильный телефон предназначен для защиты переговоров в сетях GSM. Телефон обеспечивает высокий уровень безопасности и качественный кодек голоса. Прост в использовании. Рекомендо-

ван немецким агентством по информационной безопасности.

**Технические характеристики:**

- GSM 900/1800.
- Отображение защищенного режима на дисплее.
- Вес: 105 г.
- Размеры: 118×46×21 мм.
- Питание: 3,6 В.

### Акустический сейф «Ладья»

Акустический сейф предназначен для защиты речевой информации, циркулирующей в местах пребывания владельца сотового телефона в случае его активации с целью прослушивания.

«Ладья» гарантирует защиту владельца сотового телефона от негласного прослушивания через каналы сотовой связи путем несанкционированной активации его аппарата в режиме удаленного доступа.

Защита обеспечивается путем автоматического акустического зашумления тракта передачи речевой информации при попытке дистанционного включения микрофона трубки сотового телефона.

Трубка сотового телефона помещается в настольную подставку для карандашей. В случае негласной дистанционной активации телефона в режиме прослушивания единственным демаскирующим признаком является изменение напряженности электромагнитного поля (поскольку передатчик сотового телефона несанкционированно включается на передачу). Это изменение фиксируется индикатором поля, входящим в состав устройства, который дает команду на автоматическое включение акустического шумогенератора, расположенного внутри объема изделия «Ладья». Уровень акустического шума на входе микрофона трубки сотового телефона таков, что обеспечивается гарантированное закрытие всего тракта передачи речевой информации.

Изделие «Ладья» прошло сертификационные испытания по требованиям ФСТЭК РФ (Сертификат № 698/1) и может использоваться в выделенных помещениях до 1-й категории включительно. Используемая в изделии технология защищена патентом РФ № 2183914.

**Технические характеристики модели:**

| | |
|---|---|
| Уровень шума в точке размещения микрофона сотового телефона | не менее 100 Дб |
| Эффективный спектр шумового сигнала | 250 – 4000 Гц |
| Питание изделия «Ладья» | две батареи типа AAA |
| Время непрерывной работы от одного комплекта батарей | не менее 6 месяцев |

### Акустический сейф с селекцией угроз «Свирель»

Изделие «Свирель» предназначено для активной защиты при несанкционированном включении режима прослушивания телефона оператором сотовой связи, регистрации и протоколирования обмена информацией по радиоканалу. Принцип действия изделия основан на постоянном мониторинге и анализе скрытного информационного обмена между трубкой сотового телефона и базовой станцией. Селекция типов угроз осуществляется по характеру (длительности и периодичности) импульсов скрытного информационного обмена. Информация фиксируется и выводится либо на ЖК-дисплей, либо сбрасывается через RS-232 на «PC».

**Основные характеристики терминальной программы для PC**

- графический интерфейс пользователя в стандарте Windows;
- возможность считывания протокола наблюдений или заданной его части из устройства;
- архивация протокола наблюдений;
- графическое отображение протокола наблюдений для детального анализа в виде временных диаграмм с комментариями;
- сортировка протокола по выбранным параметрам (тип события, время события и т. д.);
- обработка информации для составления файла отчета в графическом или текстовом формате;
- архивация и печать файла отчета.

### Скремблер GUARD GSM

Специально разработанный скремблер GUARD GSM, будучи эконом-вариантом, отлично замаскирует вашу речь, передаваемую по каналам GSM-связи, тем самым защищая ваши разговоры от про-


слушивания. Данное устройство соединяется с сотовым телефоном по проводной гарнитуре и имеет небольшие размеры. Скремблер GUARD GSM имеет тридцать два режима скремблирования.

Принцип работы данного скремблера основан на первоначальном разрушении и временной перестановке звука на передающей стороне с его последующим восстановлением на принимающей стороне. Этот процесс двухсторонний.

Временная перестановка отрезков речевого сигнала и восстановление их последовательности на приеме занимают некоторый интервал времени. Поэтому обязательным свойством такой аппаратуры является небольшая задержка сигнала на приемной стороне.

Начало разговора, как правило, начинается в открытом режиме и далее, по обоюдной команде, устройства переключаются в режим скремблирования. При ведении переговоров прибор выполняет одновременно две функции: скремблирование и дескремблирование. То есть произнесенная одним из абонентов речь шифруется с его стороны, а второй скремблер, находящийся у второго абонента, расшифровывает данную речь. И то же самое происходит в обратном направлении, когда начинает говорить второй абонент.

**Технические характеристики**

| | | |
|---|---|---|
| 1 | Разборчивость речи | не менее 95 % |
| 2 | Тип соединения | полный дуплекс |
| 3 | Задержка сигнала в линии | не более 100 мс |
| 4 | Уровень защищенности линейного сигнала | временный |
| 5 | Использование в сетях стандарта | GSM 900/1800 |
| 6 | Тип подключения к сотовому телефону | проводная гарнитура |
| 7 | Габаритные размеры | 80 × 45 × 16 мм |

### Скремблер «GUARD Bluetooth»

Скремблер GUARD-Bluetooth — это прибор с высоким уровнем скремблирования. Он предназначен для шифрования разговоров, ведущихся по сотовой связи. Защита информации, передаваемой по каналам сотовой связи, обеспечивается за счет первоначального разрушения спектра речи и ее временной перестановки на передающей стороне (у того абонента, который говорит).

Иначе говоря, в эфир выдаются перестановленные местами части слов. Подключившиеся к вашему разговору третьи лица, соответ-

ственно, слушают или записывают именно искаженную, не подлежащую разбору речь. Однако имеющийся у второго абонента с тем же режимом шифрования скремблер является дескремблером, который восстанавливает зашифрованную речь. Люди, ведущие разговор с использованием скремблеров, спокойно понимают друг друга.


Скремблер подсоединяется к мобильному телефону по Bluetooth и в отличие от моделей «GUARD GSM» и «GUARD Sky Link» не привязан к определенным моделям телефонов. В данном случае для обеспечения связи между скремблером и телефоном необходимо наличие функции Bluetooth соединения.

**Технические характеристики**

| | | |
|---|---|---|
| 1 | Максимальная дальность связи между скремблером «GUARD Bluetooth» и телефоном | до 6 метров |
| 2 | Максимальное время заряда встроенного LI-tON аккумулятора | до 10 часов |
| 3 | Время работы скремблера «GUARD Bluetooth» с полностью заряженным аккумулятором | до 10 часов |
| 4 | Выходная мощность передатчика «GUARD Bluetooth» | 1 мВт |
| 5 | Габаритные размеры | 90 × 50 × 18 |

## Защищенный от прослушивания телефон компании «Мегафон»

Вслед за компанией МТС, объявившей о выпуске недорогого сотового телефона под собственной торговой маркой, аналогичное заявление сделал другой федеральный оператор — «Мегафон». Новый телефон, разработанный компанией совместно с научно-техническим центром «Атлас» и получивший название «SMP-Атлас», предназначен для работы только в сетях «Мегафона» и, в отличие от представленного аппарата МТС, являющегося самым обычным телефоном, поддерживает дополнительное шифрование голосового трафика.

Шифрование голоса осуществляется в соответствии с ГОСТ 2814789, длина ключа шифрования — 256 разрядов. В телефоне реализован уникальный голосовой кодек с линейным предсказанием, скорость — 4,8 Кбит/с. Кодек, как и шифратор и другие вычислительные блоки, основан на процессоре TI TMS320C5xx.

Другая особенность новой разработки — использование для передачи речи не голосового канала, а канала передачи данных. Однако новый аппарат может работать и как обычный сотовый GSM-телефон. Как отмечает «Сотовик», предлагаемая услуга конфиденциальной связи доступна не только в сети «Мегафон», но и в сетях роуминговых партнеров оператора.

По своим функциональным возможностям «SMP-Атлас» соответствует модели Siemens C35. Его масса — 130 г, время работы в режимах разговор/ожидание соответственно 210 мин/75 часов. В защищенном режиме время разговора несколько меньше — до 180 минут. Стоимость модели — 2700 долларов. Для подключения услуги «Конфиденциальная сотовая связь» достаточно выбрать тарифный план из стандартного набора тарифов «Мегафона». Оплата трафика в защищенном режиме аналогична тарификации открытого режима.

Ключ шифрования абонент самостоятельно сменить не сможет. Если вскрыть аппарат, он автоматически заблокируется. Выданный ключ действует в течение года. Новая модель должна привлечь корпоративных клиентов и может стать вторым телефоном для спецсвязи. Злоумышленники на закрытый канал могут не рассчитывать — благодаря СОРМ вся информация доступна для компетентных органов.

### Криптосмартфон – телефон с защитой разговора

На выставке CeB1T 2006, которая состоялась в марте 2006 года, Hannover, Германия, демонстрация специально разработанного компанией АНКОРТ криптосмартфона произвела настоящую сенсацию. На крупнейшей в мире выставке по электронике и компьютерам не было ни одного подобного устройства с такой суперкриптографической защитой. Конкурирующие фирмы Германии, Италии, Швеции, Англии представили криптоGSM-телефоны, разработанные на базе обычных серийно выпускаемых GSM-аппаратов.

Криптосмартфон ANCORT A-7 обеспечит вам высочайшую защиту вашего телефонного

разговора. Для обеспечения надежной криптографической связи необходимо иметь минимум два криптосмартфона ANCORT A-7.

- Операционная система — Windows CE
- Главный процесор — Motorola MX21 (266 MHz)
- Memory — 64 Мб (Flash)/64 Мб (RAM)
- Сеть — GSM 900/1800
- Тип дисплея — Цветной TFT (262,144 цветов)
- Размер активного дисплея — 2,2" (33,84 × 45,12 мм)
- Разрешение — 240 × 320 пикс.
- Антенна — Встроенная
- Клавиатура — Латинский и Русский алфавит
- Виртуальная клавиатура — Да
- SIM-карта — Стандартная (Plug-in (3 В) type)
- Аккумулятор — 1350 mAh (Li-Polymer)
- Работа в режиме ожидания — > 100 часов
- Работа в режиме разговора — > 2 часов
- Размеры (В × Ш × Г) — 115 × 53 × 24 мм
- Вес — 150 гр
- Цвет корпуса — Серый
- SMS — Да
- MMS — Да
- E-mail — Да
- Internet — Да
- WAP 2.0 — Да
- GPRS Class 10 — Да
- JAVA support — Да
- Modem — Да
- Синхронизация — с PC Microsoft® ActiveSync®
- Интерфейс синхронизации — USB
- Количество предустановленных мелодий — 29
- Просмотр документов — Microsoft® Word
- Медиаплеер — Wav, MP3
- Загрузка мелодий и логотипов — WAP, Internet, USB
- Вибровызов — Да
- Телефонная книжка — 4000 номеров
- Количество номеров на одного абонента — 5 номеров тел. + факс и E-mail
- Количество групп в телефонной книге — 26
- Назначение мелодий — Каждому абоненту
- Система быстрого ввода текста — Да
- Календарь/Органайзер — Да
- Кнопки быстрого вызова программ — Да

- Зарядка аккумулятора
- От зарядного устройства 220 вольт
- От персонального компьютера через USB

**Комплект**

- Криптосмартфон,
- зарядное устройство,
- аккумулятор,
- синхронизация с PC (кабель и CD с программным обеспечением),
- руководство,
- гарантийный талон,
- чехол.

**Криптографические характеристики**

- Криптопроцессор — TMS 320 VC 5416
- Криптозвонок — Да
- Крипто SMS — Да
- Крипто E-mail — Да (шифруются текст и вложения)
- Кнопка криптозвонка — Отдельная кнопка
- Ключевая мощность — 1077
- Криптоалгоритм — ГОСТ 28147 – 89
- Метод распределения ключей — Открытый ключ длиной 256 бит, основан на расчете параметров эллиптических кривых
- Шифрация данных в криптосмартфоне — Да
- Слоговая разборчивость — 87%

Разработанный криптосмартфон компанией АНКОРТ имеет высочайшие криптографические, инженерно-криптографические характеристики, что обеспечивает надежную криптографическую защиту.

# Контрольные вопросы (билеты) по теме «Защита информации»

**Билет № 1**

| | | | |
|---|---|---|---|
| 1 | Коммерческая тайна — это информация, которая имеет потенциальную или действительную коммерческую ценность в силу ее неизвестности третьим лицам. | Да | Нет |
| 2 | Сведения о численности сотрудников и системе оплаты труда не могут составлять коммерческую тайну. | Да | Нет |
| 3 | Направленный микрофон — это средство перехвата информации по акустическому каналу. | Да | Нет |
| 4 | Каналы утечки информации подразделяются на акустический, вибрационный, электромагнитный и радиоканал. | Да | Нет |
| 5 | Кража документов занимает второе место среди основных видов потерь информации. | Да | Нет |
| 6 | К техническим мероприятиям по защите информации относятся: внутриобъектовый режим, инженерно-техническое оборудование объекта и оперативно-технический осмотр. | Да | Нет |
| 7 | Наибольшее количество закладок обнаруживается при проверке электронных приборов. | Да | Нет |
| 8 | Прибор «Оберег» — это радиочастотный сканер. | Да | Нет |
| 9 | Сотрудники охраны могут самостоятельно проводить визуальный осмотр и проверку ограждающих конструкций. | Да | Нет |
| 10 | При получении сведений об утечке информации сотрудники охраны должны: 1) определить примерное время внедрения; 2) определить место установки техники. | Да | Нет |
| 11 | Комплекс мероприятий по защите информации включает в себя мероприятия кадрового, организационного и технического характера. | Да | Нет |
| 12 | Жучки — это приборы для перехвата информации по электромагнитному каналу. | Да | Нет |

**Билет № 2**

| | | | |
|---|---|---|---|
| 1 | Коммерческая тайна — это информация, которая имеет потенциальную или действительную коммерческую ценность в силу отсутствия доступа к ней на законном основании | Да | Нет |
| 2 | Сведения о составе сотрудников и системе оплаты труда могут составлять коммерческую тайну. | Да | Нет |
| 3 | Направленные микрофоны бывают параболическими и плоскими. | Да | Нет |
| 4 | Каналы утечки информации подразделяются на акустический, вибрационный, электромагнитный и электрический. | Да | Нет |
| 5 | Персонал занимает второе место среди основных видов потерь информации. | Да | Нет |
| 6 | К техническим мероприятиям по защите информации относятся: внутриобъектовый режим, инженерно-техническое оборудование объекта и оперативно-технический осмотр. | Да | Нет |
| 7 | Наибольшее количество закладок обнаруживается при проверке электронных приборов. | Да | Нет |
| 8 | Прибор «Лидер» предназначен для поиска радиозакладок и мобильных телефонов. | Да | Нет |
| 9 | Сотрудники охраны могут самостоятельно проводить визуальный осмотр и контроль радиоэфира. | Да | Нет |
| 10 | При получении сведений об утечке информации сотрудники охраны должны: 1) определить примерное время внедрения; 2) определить место установки техники. | Да | Нет |
| 11 | Комплекс мероприятий по защите информации включает в себя мероприятия организационного и технического характера. | Да | Нет |
| 12 | Нелинейный локатор предназначен для перехвата информации по радиоканалу. | Да | Нет |

**Билет № 3**

| | | | |
|---|---|---|---|
| 1 | Коммерческая тайна — это информация, которая имеет потенциальную или действительную коммерческую ценность в силу ее неизвестности третьим лицам, отсутствия доступа к ней на законном основании и введении в отношении ее режима коммерческой тайны. | Да | Нет |
| 2 | Сведения, указанные в учредительных документах, не могут составлять коммерческую тайну. | Да | Нет |
| 3 | Аппаратура высокочастотного навязывания — это средство перехвата информации по акустическому каналу. | Да | Нет |
| 4 | Каналы утечки информации подразделяются на акустический, вибрационный, электромагнитный, электрический и оптический. | Да | Нет |
| 5 | Кража документов занимает второе место среди основных видов потерь информации. | Да | Нет |
| 6 | К организационным мероприятиям по защите информации в том числе относятся: пропускной режим, анализ информации в прессе и документооборот. | Да | Нет |
| 7 | Наибольшее количество закладок обнаруживается при визуальном осмотре. | Да | Нет |
| 8 | Прибор «Оберег» — это индикатор частоты. | Да | Нет |
| 9 | Сотрудники охраны могут самостоятельно проводить контроль радиоэфира и проверку электроприборов. | Да | Нет |
| 10 | При получении сведений об утечке информации сотрудники охраны должны: 1) определить примерное время внедрения; 2) сопоставить с событиями в этот период; 3) определить место установки техники. | Да | Нет |
| 11 | Комплекс мероприятий по защите информации включает в себя мероприятия кадрового и технического характера. | Да | Нет |
| 12 | «Лидер» — это прибор для поиска оптики. | Да | Нет |

**Билет № 4**

| | | | |
|---|---|---|---|
| 1 | Коммерческая тайна — это информация, которая имеет потенциальную или действительную коммерческую ценность в силу введения в отношении ее режима коммерческой тайны. | Да | Нет |
| 2 | Сведения о состоянии пожарной безопасности объекта не могут составлять коммерческую тайну. | Да | Нет |
| 3 | Бинокли, видеокамеры и тепловизоры — это средства перехвата информации по оптическому каналу. | Да | Нет |
| 4 | Каналы утечки информации подразделяются на акустический, индукционный, электромагнитный, оптический и электрический. | Да | Нет |
| 5 | При проведении контроля радиоэфира в качестве источника звука применяется метроном или радиоприемник. | Да | Нет |
| 6 | К техническим мероприятиям по защите информации относятся: изучение объекта, инженерно-техническое оборудование объекта и оперативно-технический осмотр. | Да | Нет |
| 7 | Наибольшее количество закладок обнаруживается во время контроля радиоэфира. | Да | Нет |
| 8 | Прибор «AR −8000» — это радиочастотный сканер. | Да | Нет |
| 9 | Сотрудники охраны могут частично проводить проверку электронных приборов, предметов мебели и интерьера. | Да | Нет |
| 10 | При получении сведений об утечке информации сотрудники охраны должны: 1) определить примерное время внедрения; 2) определить место установки техники. | Да | Нет |
| 11 | Комплекс мероприятий по защите информации состоит из мероприятий технического характера. | Да | Нет |
| 12 | Двери, оконные стекла, технологические проемы представляют собой акустический канал. | Да | Нет |

**Билет № 5**

| | | | |
|---|---|---|---|
| 1 | Коммерческая тайна — это информация, которая имеет потенциальную или действительную коммерческую ценность в силу отсутствия к ней доступа. | Да | Нет |
| 2 | Трубы инженерных коммуникаций представляют собой вибрационный канал утечки информации. | Да | Нет |
| 3 | Электронный стетоскоп — это средство перехвата информации по акустическому каналу. | Да | Нет |
| 4 | Каналы утечки информации подразделяются на акустический, вибрационный и электромагнитный. | Да | Нет |
| 5 | Прослушивание телефонов занимает первое место среди основных видов потерь информации. | Да | Нет |
| 6 | К техническим мероприятиям по защите информации относятся: пропускной режим, инженерно-техническое оборудование объекта и оперативно-технический осмотр. | Да | Нет |
| 7 | «Скорпион» — это прибор для поиска миниатюрных видеокамер. | Да | Нет |
| 8 | Метроном — это прибор для поиска радиомикрофонов. | Да | Нет |
| 9 | Сотрудники охраны могут самостоятельно проводить визуальный осмотр. | Да | Нет |
| 10 | При изучении объекта в том числе устанавливается: расположение категорированных помещений, факты проведения ремонтных работ, состав сотрудников охраны. | Да | Нет |
| 11 | Оперативно-технический осмотр бывает демонстративным и конспиративным. | Да | Нет |
| 12 | Жучки — это приборы для перехвата информации по акустическому каналу. | Да | Нет |

**Ответы**
**к билетам по теме «Защита информации»**

| № билета / № вопроса | Билет 1 | Билет 2 | Билет 3 | Билет 4 | Билет 5 |
|---|---|---|---|---|---|
| 1 | Нет | Нет | Да | Нет | Нет |
| 2 | Да | Нет | Да | Да | Да |
| 3 | Да | Да | Нет | Да | Нет |
| 4 | Нет | Нет | Нет | Нет | Нет |
| 5 | Нет | Нет | Нет | Нет | Нет |
| 6 | Нет | Нет | Да | Да | Нет |
| 7 | Нет | Да | Да | Нет | Да |
| 8 | Нет | Нет | Да | Да | Да |
| 9 | Нет | Да | Нет | Да | Да |
| 10 | Нет | Нет | Да | Нет | Нет |
| 11 | Нет | Да | Нет | Нет | Да |
| 12 | Нет | Нет | Да | Нет | Да |

# Приложение 1

**Федеральный закон Российской Федерации**
**от 27 июля 2006 г. № 152-ФЗ О персональных данных.**
**Опубликовано 29 июля 2006 г.**
**Вступает в силу 8 августа 2006 г.**
**Принят Государственной Думой 8 июля 2006 года.**
**Одобрен Советом Федерации 14 июля 2006 года**

## Глава 1

## ОБЩИЕ ПОЛОЖЕНИЯ

### Статья 1
### СФЕРА ДЕЙСТВИЯ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее — государственные органы), органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами (далее — муниципальные органы), юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.
2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

— обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
— организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
— обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с зако-

нодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

**Статья 2**
**ЦЕЛЬ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА**

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

**Статья 3**
**ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ФЕДЕРАЛЬНОМ ЗАКОНЕ**

В целях настоящего Федерального закона используются следующие основные понятия:
- персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;
- обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;
- использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях

принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;
- блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- информационная система персональных данных — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;
- трансграничная передача персональных данных — передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;
- общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Статья 4**

**ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

- Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федера-

ции и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

— На основании и во исполнение федеральных законов государственные органы в пределах своих полномочий могут принимать нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных. Нормативные правовые акты по отдельным вопросам, касающимся обработки персональных данных, не могут содержать положения, ограничивающие права субъектов персональных данных.

Указанные нормативные правовые акты подлежат официальному опубликованию, за исключением нормативных правовых актов или отдельных положений таких нормативных правовых актов, содержащих сведения, доступ к которым ограничен федеральными законами.

— Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

— Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

## Глава 2

## ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

### Статья 5
### ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Обработка персональных данных должна осуществляться на основе принципов:

— законности целей и способов обработки персональных данных и добросовестности;

— соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

— соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

— достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных дан-

ных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

**Статья 6**
**УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.
2. Согласие субъекта персональных данных, предусмотренное частью 1 настоящей статьи, не требуется в следующих случаях:
   1. Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
   2. Обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
   3. Обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
   4. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
   5. Обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;
   6. Обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при

условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7. Осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

3. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.
4. В случае, если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

**Статья 7**
**КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.
2. Обеспечение конфиденциальности персональных данных не требуется:
   - в случае обезличивания персональных данных;
   - в отношении общедоступных персональных данных.

**Статья 8**
**ОБЩЕДОСТУПНЫЕ ИСТОЧНИКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.
2. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по

решению суда или иных уполномоченных государственных органов.

**Статья 9**
**СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных частью 2 настоящей статьи. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.
2. Настоящим Федеральным законом и другими федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.
4. В случаях, предусмотренных настоящим Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:
   - фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
   - наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
   - цель обработки персональных данных;
   - перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
   - перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва.

5. Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительное согласие не требуется.
6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.
7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

**Статья 10**
**СПЕЦИАЛЬНЫЕ КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

- Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.
- Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:
  - субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
  - персональные данные являются общедоступными;
  - персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;
  - обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
  - обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в со-

ответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

— обработка персональных данных необходима в связи с осуществлением правосудия;

— обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

- Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.
- Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

**Статья 11**
**БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

1. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.
2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

**Статья 12**
**ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ**

- До начала осуществления трансграничной передачи персональных данных оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.
- Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.
- Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:
  - наличия согласия в письменной форме субъекта персональных данных;
  - предусмотренных международными договорами Российской Федерации по вопросам выдачи виз, а также международными договорами Российской Федерации об оказании правовой помощи по гражданским, семейным и уголовным делам;
  - предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

**Статья 13**
**ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННЫХ ИЛИ МУНИЦИПАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

- Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с феде-

ральными законами, государственные или муниципальные информационные системы персональных данных.

- Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.
- Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.
- В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

## Глава 3

## ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

### Статья 14
### ПРАВО СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ДОСТУП К СВОИМ ПЕРСОНАЛЬНЫМ ДАННЫМ

1. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными, за исключением случаев, предусмотренных частью 5 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае,

если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.
3. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.
4. Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:
   - подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
   - способы обработки персональных данных, применяемые оператором;
   - сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
   - перечень обрабатываемых персональных данных и источник их получения;
   - сроки обработки персональных данных, в том числе сроки их хранения;
   - сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.
5. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:
   1) Обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) Обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
3) Предоставление персональных данных нарушает конституционные права и свободы других лиц.

**Статья 15**

**ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ ПРОДВИЖЕНИЯ ТОВАРОВ, РАБОТ, УСЛУГ НА РЫНКЕ, А ТАКЖЕ В ЦЕЛЯХ ПОЛИТИЧЕСКОЙ АГИТАЦИИ**

— Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.
— Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в части 1 настоящей статьи.

**Статья 16**

**ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРИНЯТИИ РЕШЕНИЙ НА ОСНОВАНИИ ИСКЛЮЧИТЕЛЬНО АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

— Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.
— Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагиваю-

щее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

— Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

— Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение семи рабочих дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

**Статья 17**

**ПРАВО НА ОБЖАЛОВАНИЕ ДЕЙСТВИЙ ИЛИ БЕЗДЕЙСТВИЯ ОПЕРАТОРА**

— Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

— Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

## Глава 4

## ОБЯЗАННОСТИ ОПЕРАТОРА

**Статья 18**

**ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ СБОРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

— При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию,

предусмотренную частью 4 статьи 14 настоящего Федерального закона.

- Если обязанность предоставления персональных данных установлена федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.
- Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если персональные данные являются общедоступными, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящим Федеральным законом права субъекта персональных данных.

**Статья 19**

**МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ**

- Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
- Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.
- Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации в соответствии с частью 2 настоящей статьи, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техниче-

ским разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

– Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

**Статья 20**

**ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАЩЕНИИ ЛИБО ПРИ ПОЛУЧЕНИИ ЗАПРОСА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ЕГО ЗАКОННОГО ПРЕДСТАВИТЕЛЯ, А ТАКЖЕ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ**

– Оператор обязан в порядке, предусмотренном статьей 14 настоящего Федерального закона, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

– В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

– Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность озна-

комления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

— Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса.

**Статья 21**

**ОБЯЗАННОСТИ ОПЕРАТОРА ПО УСТРАНЕНИЮ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА, ДОПУЩЕННЫХ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ ПО УТОЧНЕНИЮ, БЛОКИРОВАНИЮ И УНИЧТОЖЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ**

— В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

— В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

— В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных наруше-

ний оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

- В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.
- В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

**Статья 22**
**УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.
2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:
   - относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;
   - полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не

предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;
- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

3. Уведомление, предусмотренное частью 1 настоящей статьи, должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации. Уведомление должно содержать следующие сведения:
   - наименование (фамилия, имя, отчество), адрес оператора;
   - цель обработки персональных данных;
   - категории персональных данных;
   - категории субъектов, персональные данные которых обрабатываются;

— правовое основание обработки персональных данных;
— перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
— описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
— дата начала обработки персональных данных;
— срок или условие прекращения обработки персональных данных.

4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.
5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.
6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.
7. В случае изменения сведений, указанных в части 3 настоящей статьи, оператор обязан уведомить об изменениях уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений.

## Глава 5

## КОНТРОЛЬ И НАДЗОР ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА

### Статья 23
### УПОЛНОМОЧЕННЫЙ ОРГАН ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контро-

ля и надзора за соответствием обработки персональных данных требованиям настоящего Федерального закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.
3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:
   - запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
   - осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
   - требовать от оператора уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;
   - принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;
   - обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;
   - направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;
   - направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

- вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;
- привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.
5. Уполномоченный орган по защите прав субъектов персональных данных обязан:
   1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;
   2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;
   3) вести реестр операторов;
   4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;
   5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;
   6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;
   7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.
6. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.
7. Уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Фе-

дерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации.

8. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.
9. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

**Статья 24**

**ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА**

Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

## Глава 6

## ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

**Статья 25**

- Настоящий Федеральный закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.
- После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.
- Информационные системы персональных данных, созданные до дня вступления в силу настоящего Федерального закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года.
- Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключени-

ем случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2008 года.

Президент Российской Федерации
В. Путин

# Приложение 2

**Федеральный закон Российской Федерации**
**от 29 июля 2004 г. № 98-ФЗ О коммерческой тайне**
**Опубликовано 5 августа 2004 г.**
**Вступает в силу с 16 августа 2004 г.**
**Принят Государственной Думой 9 июля 2004 года.**
**Одобрен Советом Федерации 15 июля 2004 года**

**Статья 1**
**ЦЕЛИ И СФЕРА ДЕЙСТВИЯ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА**

- Настоящий Федеральный закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.
- Положения настоящего Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.
- Положения настоящего Федерального закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

**Статья 2**
**ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ О КОММЕРЧЕСКОЙ ТАЙНЕ**

Законодательство Российской Федерации о коммерческой тайне состоит из Гражданского кодекса Российской Федерации, настоящего Федерального закона, других федеральных законов.

**Статья 3**
**ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ФЕДЕРАЛЬНОМ ЗАКОНЕ**

Для целей настоящего Федерального закона используются следующие основные понятия:

1. Коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
2. Информация, составляющая коммерческую тайну, — научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;
3. Режим коммерческой тайны — правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности;
4. Обладатель информации, составляющей коммерческую тайну, — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;
5. Доступ к информации, составляющей коммерческую тайну, — ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;
6. Передача информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;
7. Контрагент — сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;
8. Предоставление информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функции;

9. Разглашение информации, составляющей коммерческую тайну, — действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

**Статья 4**

**ПРАВО НА ОТНЕСЕНИЕ ИНФОРМАЦИИ К ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, И СПОСОБЫ ПОЛУЧЕНИЯ ТАКОЙ ИНФОРМАЦИИ**

- Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.
- Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом несмотря на то, что содержание указанной информации может совпадать с содержанием информации, составляющей коммерческую тайну, обладателем которой является другое лицо.
- Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.
- Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

**Статья 5**

**СВЕДЕНИЯ, КОТОРЫЕ НЕ МОГУТ СОСТАВЛЯТЬ КОММЕРЧЕСКУЮ ТАЙНУ**

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

- Содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- Содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- О составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- О загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- О численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;
- О задолженности работодателем по выплате заработной платы и по иным социальным выплатам;
- О нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- Об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- О размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- О перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

**Статья 6**

**ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ**

1. Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправ-

ления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

2. В случае отказа обладателя информации, составляющей коммерческую тайну, предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления, данные органы вправе затребовать эту информацию в судебном порядке.
3. Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию в соответствии с частью 1 настоящей статьи, обязаны предоставить эту информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.
4. На документах, предоставляемых указанным в частях 1 и 3 настоящей статьи органам и содержащих информацию, составляющую коммерческую тайну, должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

**Статья 7**
**ПРАВА ОБЛАДАТЕЛЯ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ**

- Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны в соответствии со статьей 10 настоящего Федерального закона.
- Обладатель информации, составляющей коммерческую тайну, имеет право:
  - устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

- использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;
- разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;
- вводить в гражданский оборот информацию, составляющую коммерческую тайну, на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;
- требовать от юридических и физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;
- требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществляющих случайно или по ошибке, охраны конфиденциальности этой информации;
- защищать в установленном порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

**Статья 8**

**ОБЛАДАТЕЛЬ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ПОЛУЧЕННОЙ В РАМКАХ ТРУДОВЫХ ОТНОШЕНИЙ**

- Обладатель информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений, является работодатель.
- В случае получения работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, топологии интегральной микросхемы, программы для электронных вычислительных машин или базы данных, отношения между работником и работодателем регулируются в соответствии с законодательством Российской Федерации об интеллектуальной собственности.

**Статья 9**
**ПОРЯДОК УСТАНОВЛЕНИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ ПРИ ВЫПОЛНЕНИИ ГОСУДАРСТВЕННОГО КОНТРАКТА ДЛЯ ГОСУДАРСТВЕННЫХ НУЖД**

Государственным контрактом на выполнение научно-исследовательских, опытно-конструкторских, технологических или иных работ для федеральных государственных нужд или нужд субъекта Российской Федерации должен быть определен объем сведений, признаваемых конфиденциальными, а также должны быть урегулированы вопросы, касающиеся установления в отношении полученной информации режима коммерческой тайны.

**Статья 10**
**ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ**

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:
   - определение перечня информации, составляющей коммерческую тайну;
   - ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
   - учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
   - регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
   - нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа (Коммерческая тайна) с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).
2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.
3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации,

указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.
5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:
   — исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
   — обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.
6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

**Статья 11**

**ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ И ИНФОРМАЦИИ В РАМКАХ ТРУДОВЫХ ОТНОШЕНИЙ**

1. В целях охраны конфиденциальности информации работодатель обязан:

— ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой является работодатель и его контрагенты;
— ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
— создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

2. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.
3. В целях охраны конфиденциальности информации работник обязан:

— выполнять установленный работодателем режим коммерческой тайны;
— не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;
— не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось;
— возместить причиненный работодателю ущерб, если работник виновен в разглашении информации, составляющей коммерческую тайну, ставшей ему известной в связи с исполнением им трудовых обязанностей;
— передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.

4. Работодатель вправе потребовать возмещения причиненных убытков лицом, прекратившим с ним трудовые отношения, в случае, если это лицо виновно в разглашении информации, составляющей коммерческую тайну, доступ к которой это лицо получило в связи с исполнением им трудовых обязанностей, если разглашение такой информации последовало в течение срока, установленного в соответствии с пунктом 3 части 3 настоящей статьи.
5. Причиненные ущерб либо убытки не возмещаются работником или прекратившим трудовые отношения лицом, если разглашение информации, составляющей коммерческую тайну, явилось следствием непреодолимой силы, крайней необходимости или неисполнения работодателем обязанностей по обеспечению режима коммерческой тайны.
6. Трудовым договором с руководителем организации должны предусматриваться его обязательства по обеспечению охраны конфиденциальности информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны ее конфиденциальности.
7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тай-

не. При этом убытки определяются в соответствии с гражданским законодательством.

8. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

**Статья 12**

**ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В РАМКАХ ГРАЖДАНСКО-ПРАВОВЫХ ОТНОШЕНИЙ**

— Отношения между обладателем информации, составляющей коммерческую тайну, и его контрагентом в части, касающейся охраны конфиденциальности информации, регулируются законом и договором.

— В договоре должны быть определены условия охраны конфиденциальности информации, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору.

— В случае, если иное не установлено договором между обладателем информации, составляющей коммерческую тайну, и контрагентом, контрагент в соответствии с законодательством Российской Федерации самостоятельно определяет способы защиты информации, составляющей коммерческую тайну, переданной ему по договору.

— Контрагент обязан незамедлительно сообщить обладателю информации, составляющей коммерческую тайну, о допущенном контрагентом либо ставшем ему известном факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании информации, составляющей коммерческую тайну, третьим лицам.

— Обладатель информации, составляющей коммерческую тайну, переданной им контрагенту, до окончания срока действия договора не может разглашать информацию, составляющую коммерческую тайну, а также в одностороннем порядке прекращать охрану ее конфиденциальности, если иное не установлено договором.

— Сторона, не обеспечившая в соответствии с условиями договора охраны конфиденциальности информации, переданной по договору, обязана возместить другой стороне убытки, если иное не предусмотрено договором.

**Статья 13**
**ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ПРИ ЕЕ ПРЕДОСТАВЛЕНИИ**

- Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.
- Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей коммерческую тайну, не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных настоящим Федеральным законом, а также не вправе использовать эту информацию в корыстных или иных личных целях.
- В случае нарушения конфиденциальности информации должностными лицами органов государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством Российской Федерации.

**Статья 14**
**ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА**

- Нарушение настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.
- Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

— Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.
— Лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности.
— По требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное в части 4 настоящей статьи, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять указанные меры обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав.

**Статья 15**
**ОТВЕТСТВЕННОСТЬ ЗА НЕПРЕДСТАВЛЕНИЕ ОРГАНАМ ГОСУДАРСТВЕННОЙ ВЛАСТИ, ИНЫМ ГОСУДАРСТВЕННЫМ ОРГАНАМ, ОРГАНАМ МЕСТНОГО САМОУПРАВЛЕНИЯ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ**

Невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством Российской Федерации.

**Статья 16**
**ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ**

Грифы, нанесенные до вступления в силу настоящего Федерального закона на материальные носители и указывающие на содержание в них информации, составляющей коммерческую тайну, сохра-

няют свое действие при условии, если меры по охране конфиденциальности указанной информации будут приведены в соответствие с требованиями настоящего Федерального закона.

Президент Российской Федерации
В. Путин

# Приложение 3

## БОРЬБА С ИНСАЙДЕРАМИ — ВНУТРЕННИМИ ШПИОНАМИ

Информационная безопасность (ИБ), как известно, имеет дело с двумя категориями угроз: внешними и внутренними. Именно к последнему типу относятся инсайдеры. Их деятельность в большинстве случаев неумышленна, и именно поэтому ее трудно предугадать и обезвредить. Для этого надо задействовать весь арсенал доступных средств ИБ.

Существующая в настоящее время индустрия информационной безопасности (ИБ), обороты которой составляют десятки миллиардов долларов, развивается в основном на волне противодействия внешним угрозам, обязанным своим появлением прорыву в области высоких технологий, Интернет и электронной коммерции. Одним из первых и фундаментальных механизмов защиты от внешней угрозы стал межсетевой экран, постепенно «обросший» системами обнаружения вторжений, средствами VPN и фильтрации контента. Наряду с межсетевыми экранами активно развивались и продолжают развиваться другие средства обеспечения сетевой и хостовой безопасности: системы мониторинга и аудита событий, средства защиты от вредоносного ПО, средства аутентификации и контроля доступа, криптографические и другие средства, работающие на предотвращение несанкционированного доступа к информации.

Наиболее распространенные каналы утечки относятся к категории неумышленного раскрытия по причине неосведомленности или недисциплинированности. Это:

- банальная «болтовня сотрудников»;
- отсутствие представлений о правилах работы с конфиденциальными документами;
- неумение определить, какие документы являются конфиденциальными.

Умышленный «слив информации» встречается значительно реже, зато в данном случае информация «сливается» целенаправленно и с наиболее опасными последствиями для организации.

Инсайдеры представляют угрозу, прежде всего, для интеллектуальной собственности организации — одного из ее основных активов. Установление и защита прав на интеллектуальную собственность в настоящее время является важнейшим аспектом любого

бизнеса, в особенности малого, являющегося, как известно, оплотом любой здоровой экономики.

## КТО УГРОЖАЕТ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ?

Чтобы выжить на рынке, бизнесу нужно уметь справляться с целой армией разного рода конкурентов. Майкл Лектер в своей книге «Защити свой главный актив» подразделяет их на три категории: «большие парни», «спойлеры» и «пираты».

Оружием инсайдера может стать любой носитель информации, например простая флешка.

**«Большие парни»** — это конкуренты, прочно закрепившиеся на рынке. Они располагают значительными финансовыми ресурсами и вкладывают их в маркетинг, исследования и разработки. Они могут получать значительные преимущества от масштабов ведения дела, используя стабильные каналы сбыта, налаженные взаимоотношения с партнерами и хорошую репутацию у потребителей. Хотя «большие парни» обычно проявляют особую щепетильность относительно чужих законных прав на интеллектуальную собственность, они воспользуются любым пробелом в этой области, чтобы обернуть его в свою пользу и попытаться сокрушить конкурента при помощи денег и силы, которой они обладают на рынке.

**«Спойлеры»** — это конкуренты, представляющие на рынке менее дорогие и худшие по качеству варианты продукции. Они могут сбить цены или вообще разрушить рынок компании. «Спойлер» старается не замечать прав на интеллектуальную собственность, но, получив отпор, научится проявлять к ним уважение.

**«Пираты»** — это неразборчивые в средствах ребята. Пренебрегая правами на интеллектуальную собственность, они сознательно копируют продукцию или создают путаницу на рынке, сбывая свой товар под видом чужого. Они будут присваивать инвестиции, сделанные в продукцию и товарный знак до тех пор, пока их не остановят.

Существуют различные законные и не очень методы конкурентной разведки, но попадает конфиденциальная информация к этим парням, главным образом, через инсайдеров. Это и «халатные» сотрудники, выносящие информацию из офиса для работы с ней дома или в командировке с последующей утерей этой информации, и «жертвы социальной инженерии», дублирующие конфиденциальную информацию на почтовый ящик мошенника, и «обиженные», стремящиеся скомпрометировать работодателя любым способом, и «нелояльные», мечтающие поскорее сменить место работы, прихватив с собой корпоративные ноу-хау, и подрабатывающие или

специально внедренные «инсайдеры», передающие секретные планы слияний и поглощений недобросовестным участникам фондового рынка, готовым отвалить за эту информацию «любые бабки».

Поэтому крайне важно минимизировать негативное влияние инсайдеров на бизнес организации путем своевременного их обнаружения, адекватного реагирования, предотвращения «слива» информации и применения к ним дисциплинарных и правовых мер пресечения. Для решения этой непростой задачи придется задействовать весь арсенал доступных средств, включая юридические, организационные и программно-технические механизмы защиты.

Конечно, «большие парни», «спойлеры» и «пираты» редко встречаются на рынке в чистом виде. Обычно мы имеем дело с некоторой их комбинацией. Однако, к какой бы категории ни относился конкурент, самой эффективной защитой от него является правильно заложенный законодательный фундамент прав на интеллектуальную собственность. Чтобы выжить в конкурентной борьбе, необходимо использовать всю мощь и силу государства — нашего самого главного акционера, всегда стабильно получающего свои дивиденды.

## ЮРИДИЧЕСКИЕ ИНСТРУМЕНТЫ

Использование юридических инструментов для защиты интеллектуальной собственности — единственный шанс для малого бизнеса на выживание в конкурентной борьбе с «большими парнями». Эти инструменты включают в себя патентное и авторское право, а также право на защиту товарных знаков и коммерческой тайны. Первые три инструмента используются для защиты прав интеллектуальной собственности на открытую информацию и являются самодостаточными, т. е. не требуют применения каких-либо дополнительных мер. Значительно сложнее обстоит дело с защитой коммерческой тайны, так как основной угрозой здесь является утечка информации, и обусловлена она, прежде всего, фундаментальной природой человека как носителя и распространителя информации.

При решении столь сложной проблемы как защита коммерческой тайны не удастся ограничиться одними юридическими инструментами. Эти инструменты позволяют предотвратить многие неправомерные действия со стороны конкурентов, адекватно на них отреагировать и восстановить справедливость, обрушив на противника всю мощь беспощадной государственной машины. Однако для того, чтобы привести юридические механизмы в действие, необходимо вовремя обнаружить утечку информации и собрать необходимые доказательства.

Механизмы юридической защиты коммерческой тайны могут быть запущены только при определенных условиях. Согласно закону «О коммерческой тайне», права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны, под которым понимаются «правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности».

Таким образом, помимо юридических мер по защите коммерческой тайны, заключающихся главным образом в подписании сотрудниками организации соглашений о конфиденциальности, определении положений по защите коммерческой тайны и соответствующих перечней конфиденциальной информации, должен применяться целый комплекс организационных и программно-технических мер защиты.

## СОЦИАЛЬНЫЙ МЕЖСЕТЕВОЙ ЭКРАН

Поскольку традиционные средства защиты от несанкционированного доступа оказываются малопригодными для защиты от утечки информации, здесь должны использоваться совсем иные средства, в основе которых лежит введенное кем-то из экспертов понятие «социального межсетевого экрана» (human firewall). Под этим термином понимается совокупность организационных мер информационной безопасности, направленных на работу с персоналом.

Основные принципы и правила управления персоналом с учетом требований ИБ определены в Международном стандарте ISO 17799. Они сводятся к необходимости выполнения определенных требований при найме и увольнении работников, повышения осведомленности и применения мер пресечения к нарушителям. Соблюдение этих правил позволяет существенно снизить влияние человеческого фактора, избежать характерных ошибок и, во многих случаях, предотвратить утечку и ненадлежащее использование информации.

Социальный межсетевой экран строится на фундаменте политики ИБ. В организации необходимо разработать положение по защите конфиденциальной информации и соответствующие инструкции. Эти документы должны определять правила и критерии для категорирования информационных ресурсов по степени конфиденциальности, правила маркирования и обращения с конфиденциальными сведениями. Следует определить правила предоставления доступа к информационным ресурсам, внедрить соответствующие процедуры и механизмы контроля, включая авторизацию и аудит доступа.

Для предотвращения утечек необходимо предупредить персонал о мерах, принимаемых руководством с целью защиты информации, и мерах воздействия на нарушителей политики ИБ.

Социальный межсетевой экран позволяет успешно бороться с наиболее многочисленным классом угроз — угрозами непреднамеренного разглашения конфиденциальной информации, но для борьбы со злоумышленниками его явно недостаточно. Для того чтобы остановить инсайдера, намеренно «сливающего» информацию, придется дополнительно задействовать разнообразные программно-технические механизмы защиты.

## СРЕДСТВА КОНТРОЛЯ ДОСТУПА И ПРЕДОТВРАЩЕНИЯ УТЕЧКИ ИНФОРМАЦИИ

Для ограничения доступа к информации и протоколирования фактов доступа можно использовать стандартные сервисы безопасности. К их числу относятся аутентификация, управление доступом, шифрование и аудит.

Однако традиционные схемы аутентификации и управления доступом не обеспечивают адекватного уровня защиты. В дополнение к ним целесообразно использовать специализированные сервисы управления правами доступа к электронным документам, использующиеся, например, в MS Windows Server 2003. RMS (Rights Management Services) — технология, используемая RMS-совместимыми приложениями для защиты электронных документов от несанкционированного употребления. RMS позволяет при распространении информации определять ограничения по ее использованию. Например, автор документа может ограничить «время жизни» документа, а также возможность для определенных пользователей открывать, изменять, копировать в буфер обмена, печатать или пересылать документ. Основное отличие данной технологии от традиционных способов разграничения доступа к информации заключается в том, что права доступа и дополнительные ограничения хранятся в теле самого документа и действуют независимо от его местонахождения. Шифрование документов, реализованное в технологии RMS, не позволяет получать доступ к их содержанию каким-либо обходным путем.

Для предотвращения несанкционированного копирования конфиденциальной информации на внешние носители используется специализированное программное обеспечение, предназначенное для контроля внешних коммуникационных портов компьютера (USB, IR, PCMCIA и т. п.). Эти программные продукты поставляются такими компаниями, как SecureWave, Safend, Control Guard и др.,

а также отечественными разработчиками: SmartLine и SecurIT. Пользователям присваиваются права доступа к контролируемым устройствам, по аналогии с правами доступа к файлам. В принципе, практически такого же эффекта можно добиться, используя штатные механизмы Windows, однако использование специализированного продукта все же предпочтительней, тем более что в ряде продуктов поддерживается также механизм теневого копирования данных, позволяющий дублировать информацию, копируемую пользователем на внешние устройства.

Недостатки подобных продуктов на основе статической блокировки устройств заключаются в том, что они не контролируют передачу сведений по сети и не умеют выделять конфиденциальную информацию из общего потока, работая по принципу «все или ничего». Кроме того, защиту от выгрузки программного агента такой системы, как правило, можно обойти.

Большие возможности по предотвращению утечки информации предоставляет программное обеспечение, обладающее возможностью динамически регулировать доступ к каналам передачи данных, в зависимости от уровня конфиденциальности информации и уровня допуска сотрудника. Для реализации этого принципа используется механизм мандатного управления доступом. Хозяин информационного ресурса не может ослабить требования на доступ к этому ресурсу, в его власти только усиливать их в пределах своего уровня. В таких системах конфиденциальные сведения не могут копироваться на носитель или передаваться по коммуникационному порту, имеющему более низкий уровень конфиденциальности, нежели копируемая информация. Ослаблять требования может только администратор, наделенный особыми полномочиями.

Однако системы мандатного управления доступом, как правило, дороги, сложны в реализации и оказывают существенное ограничивающее влияние на бизнес-процессы. Но самое обидное то, что, если речь идет не об особо охраняемых объектах, где на входе обыскивают, сотрудники работают по записи и все за одним компьютером, который никуда не подключен, опломбирован и не имеет внешних портов, а о реальной корпоративной среде, в которой используются ноутбуки, КПК и разнообразные каналы внешних коммуникаций, то злонамеренный инсайдер все равно найдет способ похитить информацию, поскольку он имеет к ней легальный доступ. Поэтому, в то время как нормативная база предписывает обязательное использование мандатного управления доступом в системах, имеющих дело

с государственной тайной, в корпоративной среде такие механизмы защиты применяются редко.

Средства контроля доступа и предотвращения утечки информации направлены, главным образом, на защиту от несанкционированного доступа и несанкционированного копирования информации и малоэффективны для защиты от «инсайдеров», имеющих к этой информации легальный доступ. В связи с этим в настоящее время особенно активно развивается рынок специализированных систем обнаружения и предотвращения утечек информации (Information Leakage Detection and Prevention, или сокращенно ILD&P).

## СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ

Существующие на рынке ILD&P-системы можно подразделить на сетевые, хостовые и комбинированные.

Сетевые ILD&P используются для мониторинга исходящего трафика и выявления несанкционированной передачи информации по электронной почте, в чатах, системах мгновенного обмена сообщениями и с использованием различных протоколов сети Интернет. Подобные системы начали поставляться на рынок сравнительно недавно созданными компаниями (Vericept, Vontu, PortAuthority, Tablus и др.). Они представляют собой либо анализаторы сетевого трафика, выполненные в виде аппаратных комплексов на базе Linux, либо прокси-серверы, предназначенные для анализа определенных протоколов Интернет (http, ftp и т. п.), либо почтовые шлюзы, анализирующие протоколы smtp, pop3, и imap.

Однако использование шлюзовых продуктов для обнаружения и предотвращения умышленного «слива» данных равносильно попыткам поймать шпиона путем наблюдения за его явочными квартирами и прослушивания его телефона. Эффективность этих мер невысока, т. к. явочные квартиры можно поменять, а вместо своего телефона воспользоваться другими средствами связи или другим телефоном. Поэтому продукты данного класса годятся только для создания архивов трафика и предотвращения случайной утечки информации.

Чтобы выявлять и останавливать инсайдеров-шпионов, необходимо действовать против них их же испытанным оружием, которым пользуются все спецслужбы: вести за ними постоянное наблюдение и подробно регистрировать все их действия (жучок в кармане пиджака, слежка, видеонаблюдение, скрытая камера и другие формы наблюдения). На рабочих местах и ноутбуках должно быть установлено специализированное шпионское программное обеспечение,

перехватывающее не только все формы электронных взаимодействий, но и клавиатурный набор, а также образы экрана. Это программное обеспечение должно обладать возможностями идентификации подозрительной активности пользователя (в том числе такой, которая может предшествовать «сливу» сведений) и предоставлять аналитику набор отчетов, содержащих различные срезы информации, касающейся действий над конфиденциальными базами и файлами. Скрытая слежка и непрерывный анализ всех действий потенциального злоумышленника является наиболее действенным и бескомпромиссным способом его обнаружения и нейтрализации. Рано или поздно шпион себя проявит — и вот тут надо документировать улики и юридически грамотно провести расследование.

# Оглавление

Учебное издание

**Козлов Сергей Николаевич**

**Защита информации:
устройства несанкционированного съема информации
и борьба с ними**

Корректор: Моисеева Т.Г.
Компьютерная верстка: Крылов К.А.
Группа допечатной подготовки изданий:
Зеленцов П.О.
Исакова Т.В.
Коновалова Т.Ю.
Пияева М.В.

В оформлении обложки использована картина
Алексея Беляева-Гинтовта «Звезда»

Подписано в печать 13.12.2017. Формат 60 × 90/16.
Бумага офсетная. Печать офсетная.
Усл. печ. л. 18,0. Тираж 300 экз. Заказ №

Издательство «Академический проект»
(общество с ограниченной ответственностью),
адрес: 111399, г. Москва, ул. Мартеновская, 3;
сертификат соответствия
№ РОСС RU. АЕ51. Н 16070 от 13.03.2012;
орган по сертификации РОСС RU.0001.11АЕ51
ООО «Профи-сертификат».

Отпечатано: Публичное акционерное общество
«Т8 Издательские Технологии»,
адрес: 109316, г. Москва, Волгоградский просп., 42, корп. 5,
телефон: +7 495 221 8980

**По вопросам приобретения книги
просим обращаться в издательство:**

телефоны: + 7 495 305 3702, + 7 495 305 6092,
факс: + 7 495 305 6088,
e-mail: info@aprogect.ru, zakaz@aprogect.ru,
интернет-магазин: www.academ-pro.ru.