БАШКИРСКИЙ ИНСТИТУТ СОЦИАЛЬНЫХ ТЕХНОЛОГИЙ (ФИЛИАЛ)
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ПРОФСОЮЗОВ
ВЫСШЕГО ОБРАЗОВАНИЯ
«АКАДЕМИЯ ТРУДА И СОЦИАЛЬНЫХ ОТНОШЕНИЙ»

СПЕЦИАЛЬНАЯ ТЕХНИКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

УЧЕБНОЕ ПОСОБИЕ

УФА
2017

УДК 343.98
ББК 67.52
С71

Составители: Е. Р. Пудаков, Р. Р. Яппаров

Рецензенты:
Назыров Т. В., полковник полиции, врио начальника УУР МВД по РБ;
Поезжалов В. Б., кандидат юридических наук, доцент, полковник полиции,
начальник кафедры профессиональной подготовки УЮИ МВД РФ

С71 **Специальная техника правоохранительных органов** : учебное пособие / сост. : Е. Р. Пудаков, Р. Р. Яппаров ; Башкирский институт социальных технологий (филиал) ОУП ВО «Академия труда и социальных отношений». — Уфа : изд-во БИСТ (филиал) ОУП ВО «АТиСО», 2017. — 240 с.
ISBN 978-5-904354-50-3

Учебное пособие посвящено актуальным проблемам применения специальных технических средств в правоохранительной деятельности. В данном пособии рассматриваются современные специальные средства, состоящие на вооружении различных правоохранительных органов современной России — МВД, ФССП, ФСИН и др. В нем рассмотрены тактико-технические характеристики современных специальных технических средств, поисковых технических средств, средств охраны и средств наблюдения, а также освещены основные направления технического оснащения и применения специальных химических веществ в оперативно-розыскной деятельности.

Пособие предназначено для изучения студентам направления подготовки 40.03.01 «Юриспруденция», специальности среднего профессионального обучения 40.02.02 «Правоохранительная деятельность».

УДК 343.98
ББК 67.52

ISBN 978-5-904354-50-3

Содержание

Введение 5

Тема 1. Поисковые технические средства 6
§ 1. Классификация поисковых средств 8
§ 2. Средства поисковой техники 17
§ 3. Магнитометрические средства обнаружения 21
§ 4. Технические средства поиска наркотических веществ 24
§ 5. Средства контроля и досмотра в деятельности правоохранительных органов 26

Тема 2. Современные технические средства наблюдения 29
§ 1. Системы телевизионного наблюдения 29
§ 2. Элементы систем телевизионного наблюдения 32
§ 3. Средства непосредственного наблюдения 44

Тема 3. Средства охранно-пожарной сигнализации 54
§ 1. Особенности построения и тенденции развития современных технических средств охранной сигнализации 54
§ 2. Классификация чувствительных элементов средств обнаружения 63
§ 3. Системы пожарной сигнализации 74
§ 4. Технические средства и системы защиты внешнего периметра объекта 82
§ 5. Прикладные проблемы построения систем обеспечения безопасности объектов 89

Тема 4. Технические средства контроля и управления доступом 96
§ 1. Назначение и структура систем контроля и управления доступом 96
§ 2. Элементы систем контроля и управления доступом 97

Тема 5. Техническое оснащение оперативно-розыскного производства 105
§ 1. Оперативно-розыскное производство как реализация оперативно-технических форм оперативно-розыскной деятельности 105
§ 2. Технические средства обеспечения оперативной работы 108
§ 3. Полиграф, детектор лжи 113
§ 4. Противодействие техническим средствам разведки 116

Тема 6. Специальные химические вещества 121
§ 1. Виды специальных химических веществ и их основные свойства 121
§ 2. Основные направления использования специальных химических веществ 126
§ 3. Понятие и виды химических ловушек 128
§ 4. Порядок применения химических ловушек 134
§ 5. Правовые аспекты применения химических ловушек 135

Тема 7. Технические средства защиты информации 142
§ 1. Выявление каналов утечки и несанкционированного доступа к ресурсам 142
§ 2. Технические каналы утечки акустической (речевой) информации 150

§ 3. Планирование защитных мероприятий
по видам дестабилизирующего воздействия 154
§ 4. Средства защиты информации в автоматизированных системах 161

Тема 8. Технические и организационные особенности построения и эксплуатации каналов связи 173
§ 1. Понятие и назначение систем связи 173
§ 2. Виды связи 178
§ 3. Организация и эксплуатация служебных сетей связи
органов внутренних дел 180

Тема 9. Проводные средства связи 184
§ 1. Основные понятия электросвязи, виды и характеристики
сигналов связи 184
§ 2. Виды проводных средств связи 185
§ 3. Принцип работы телефонного аппарата
и состав проводного канала связи 189

Тема 10. Средства радиосвязи 197
§ 1. Понятие радиосвязи. Основные характеристики радиосигналов 197
§ 2. Виды и особенности распространения радиоволн
различных диапазонов 200
§ 3. Состав, принцип работы и назначение элементов
радиопередающих устройств 202

Тема 11. Средства связи с мобильными объектами 206
§ 1. Классификация систем радиосвязи с мобильными объектами 206
§ 2. Состав и особенности работы средств радиотелефонной связи ОВД 218
§ 3. Порядок настройки и работы с радиотелефонными средствами 220

Тема 12. Оперативно-служебный транспорт 222
§ 1. Роль специального транспорта в решении задач по обеспечению
общественного порядка и борьбы с преступностью 222
§ 2. Виды специального транспорта и их назначение
при осуществлении различных оперативно-служебных мероприятий 222

Тема 13. Технические средства дежурных частей 225
§ 1. Назначение и виды технических средств дежурных частей 225
§ 2. Задачи, решаемые с помощью автоматизированных
информационно-управляющих систем дежурных частей 229
§ 3. Технологии функционирования дежурной части
в условиях комплексного применения технических средств 231

Тема 14. Средства усиления речи 232
§ 1. Назначение и основные направления применения средств
усиления речи в оперативно-служебной деятельности 232
§ 2. Виды средств усиления речи, их классификация 233
§ 3. Тактические особенности использования средств усиления речи 234

Список использованной литературы 237

Введение

Одной из важнейших задач развития социальной сферы является обеспечение безопасности населения. Снижения опасности для личности, семьи и общества предполагается достичь за счет принятия комплексных мер, направленных на ослабление криминогенной обстановки, повышение профессиональных возможностей государственных органов по защите правопорядка, совершенствование методов и форм борьбы с преступностью.

Специальная техника правоохранительных органов представляет собой приборы, устройства, оборудование, механизмы, химические вещества и другие созданные человеком предметы (а также способы их применения), которые могут быть правомерно и результативно использованы при проведении оперативно-розыскных мероприятий, следственных действий, поддержании режима в исправительных учреждениях, охране правопорядка с целью профилактики преступности и раскрытия преступлений в городах и других населенных пунктах.

Актуальность в применении этих средств вызвана многими причинами. Среди них — рост преступности и обострение криминогенной обстановки в большинстве регионов России, ослабление роли общественных организаций и самодеятельных объединений граждан по охране общественного порядка, усложнение задач правоохранительных органов, связанных с изменением характера и содержания преступлений и происшествий. Кроме того, осложняющим фактором являются идущие процессы реформирования ряда силовых правоохранительных структур. Все это требует внедрения новых технических средств и информационных технологий в их деятельность.

Введение и использование современных средств позволяет повысить эффективность деятельности сотрудников правоохранительной сферы, которая протекает в условиях интеллектуальной, эмоциональной и физической напряженности с ее главными отличительными особенностями: продолжительность и неравномерность рабочих нагрузок, работа с оружием, наличие стрессовых ситуаций, повышенная степень риска, что в совокупности может быть объединено понятием экстремальной ситуации и эмоционального стресса.

Успешное выполнение мероприятий, связанных с применением специальных технических средств достигается:

– твердым знанием и выполнением личным составом требований нормативных документов, регламентирующих организацию эксплуатации средств специальной техники;

– воспитанием у личного состава уверенности в боевых качествах используемых средств защиты, стремления в совершенстве знать эксплуатируемые специальные средства и необходимости постоянно поддерживать их в исправном состоянии;

– уверенным владением личным составом тактико-технических характеристик, порядка использования специальных технических средств, правил эксплуатации и обслуживания.

Тема 1. ПОИСКОВЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

В деятельности правоохранительных органов России используются разнообразные технические средства, которые позволяют решать сложные и трудоемкие задачи, связанные с обнаружением тщательно скрываемых объектов преступлений и других правонарушений. При этом объектами сокрытия могут быть следы и орудия преступлений, документы и материалы, содержащие сведения компрометирующего характера, предметы преступного посягательства и т. п., которые в ряде случаев являются основными, а иногда и единственными вещественными доказательствами. Специфика операций по поиску объектов состоит в том, что их обнаружение проводится, как правило, в условиях неполноты информации о свойствах, состоянии и местонахождении в окружающей или укрывающей среде. Для успешного решения этой задачи необходимо учитывать вид «поисковой» ситуации, под которой понимают обстановку и условия проведения поиска, а также способы сокрытия, являющиеся существенным элементом способа совершения преступления или другого нарушения режима отбывания наказания. Знание субъектом поиска типичных способов сокрытия материальных объектов и умение давать им так называемую криминалистическую характеристику в значительной мере облегчает решение конкретных поисковых задач как при проведении оперативно-розыскных мероприятий (ОРМ), так и других действий.

Сотрудники правоохранительных органов располагают широким комплексом различных технических средств, позволяющих оперативно решать конкретные задачи. Поисковые приборы предназначены, в отличие от других технических средств, таких как, например, охранная техника, для обнаружения каких-либо ***неодушевленных материальных*** объектов в укрывающей их окружающей среде. Таковыми могут быть орудия преступления (оружие, орудия взлома и др.), запрещенные предметы и ценности, небольшие предметы, укрытые в одежде, обуви, книгах и т. д. К числу этих объектов относятся и захоронения трупов людей и животных, являющихся жертвами преступлений. Современное обнаружение и изъятие указанных объектов является одним из важнейших условий предупреждения и раскрытия преступлений.

В зависимости от способа совершения преступления, вида и особенностей скрываемых объектов различают следующие способы сокрытия преступлений и других нарушений режима отбывания наказания: утаивание, маскировка, помещение объекта в специальное хранилище и смешанные.

Самым распространенным способом сокрытия является ***утаивание,*** сущность которого состоит в помещении искомых объектов в укрывающую материальную среду, препятствующую визуальному восприятию.

Под ***маскировкой*** следует понимать специальные и целенаправленные действия по созданию внешних признаков, дезинформирующих местоположение искомого объекта в окружающей или укрывающей среде, а также о действительном его назначении или содержании. Различают естественную и искусственную маскировку. Наиболее квалифицированным способом сокрытия является использование ***специальных хранилищ.***

Для повышения надежности сокрытия материальных объектов в тайниках и контейнерах довольно часто применяется ***смешанный способ сокрытия,*** т. е. разрабатываются специальные защитные меры, предотвращающие несанкционированное ознакомление случайных лиц с вложением.

Выделение поиска в самостоятельную задачу необходимо потому, что найти скрываемые объекты невозможно без обнаружения признаков, свидетельствующих об их существовании в конкретном месте обследуемой обстановки. Поэтому для эффективного разоблачения ухищрений и преодоления уловок, применяемых преступными элементами при сокрытии объектов, субъекту поиска необходимо знать закономерности возникновения и обнаружения демаскирующих признаков и уметь за обнаруженными признаками определить замаскированную сущность скрываемого объекта. Это важно при выдвижении и проверке версий относительно способов сокрытия, местоположения, свойств и состояний объектов, выборе условий проведения поиска и применения технико-криминалистических поисковых средств, а также для учета возможных негативных обстоятельств и их последствий при проведении поиска с применением этих средств.

Демаскирующие признаки возникают, как правило, в результате закономерных изменений в окружающей или укрывающей среде, а также в самом объекте при его вскрытии вследствие активного воздействия субъекта поиска или их взаимодействия друг с другом.

Демаскирующие признаки бывают прямые (основные) и косвенные (дополнительные). Прямым демаскирующим признаком является контрастность на фоне структуры среды или окружающей обстановки. Это имеет принципиальное значение, поскольку наличие у скрываемого объекта хотя бы одной качественной характеристики, отличающей его от окружающей или укрывающей среды, приводит к обнаружению искомого объекта, зачастую даже без разрушения укрывающей среды.

Наиболее существенными характеристиками, которые могут использоваться для целей обнаружения скрытых объектов, являются:

– механические (плотность, твердость, упругие и демпфирующие свойства, неоднородность и т. п.);

– электрические и магнитные (электропроводность, магнитная проницаемость и др.);

– электромагнитные (т. е. способность пропускать, отражать, преломлять и поглощать проникающие электромагнитные излучения);

– термические (теплопроводность, термическое расширение, иные изменения свойств, возникающих при перепадах температур);

– химические.

В процессе сокрытия косвенные признаки возникают при взаимодействии субъекта сокрытия, скрываемого объекта и окружающей или укрывающей среды. Необходимо отметить, что косвенные демаскирующие признаки иногда возникают и после сокрытия материальных объектов. Однако основанием для определения местоположения или назначения скрытого объекта может служить лишь совокупность прямых и косвенных признаков, поскольку возникновение косвенных признаков бывает обусловлено случайными факторами, не связанными непосредственно с действиями по сокрытию.

Известно, что объекты, подлежащие обнаружению, называются искомыми предметами (или объектами поиска), а преграды, за которыми они скрыты, — укрывающими средами. Поскольку искомые предметы по каким-либо объективным свойствам отличаются от укрывающей среды, за (в) которой они находятся, то появляется возможность использования поисковой техники.

Таким образом, ***под поисковой техникой следует понимать такие приборы, устройства и приспособления, которые позволяют обнаружить объекты,***

скрытые в укрывающих средах (грунте, воде, одежде, багаже и т. д.) по признакам, неразличимым для органов чувств человека.

Объединяет эти разнообразные средства цель их применения — обнаружение, отыскание различных материальных объектов и разнообразных по природе излучений, представляющих интерес для правоохранительных органов.

Поисковые средства широко используются в оперативно-розыскной деятельности (непроцессуальная форма), в том числе и до возбуждения уголовного дела. Факт обнаружения объектов может послужить основанием для возбуждения дела и производства расследования. В процессуальной форме поисковые средства применяются при проведении следственных действий, таких как следственный осмотр (все его виды); обыск любого вида; освидетельствование живых лиц; выемка предметов, документов и почтово-телеграфной корреспонденции; следственный эксперимент, выполняемый с целью опытной проверки показаний; эксгумация. Применение поисковых средств и полученные с их помощью результаты отражаются в протоколе соответствующего следственного действия, который удостоверяется подписями понятых и других участников.

§ 1. Классификация поисковых средств

Поисковые технические средства подразделяют по принципу их действия на несколько основных групп: средства механические, магнитные, химические, электрические, индукционные, излучающего действия и детекторы излучений.

Поисковые средства механического действия. К поисковым средствам механического действия относятся достаточно простые устройства, повышающие эффективность поиска. Для зондирования участков грунта с целью обнаружения закопанных объектов используются щупы и буры. Большой щуп, представляющий собой стержень длиной 150 см с рабочим конусным наконечником и упорной перекладиной, имеется в передвижной криминалистической лаборатории. Этот щуп позволяет проверять слои грунта на значительной глубине, отыскивать предметы под снежным покровом.

В следственный комплект включен разборный щуп; для приведения его в рабочее состояние заостренный стержень ввинчивается в рукоятку с резиновым упором. В другом варианте к рукоятке присоединяется удлинительный стержень с установленным в нем конусом (общая длина 90 см). Вариант выбирается с учетом плотности проверяемой среды.

Поиск на местности обычно начинают с выборочного зондирования, исходя из имеющейся информации о предполагаемом местонахождении объекта. Во внимание следует принимать также видимые признаки вскапывания: взрыхленная почва, увядшая растительность, провалы грунта и т. п.

Если выборочное зондирование не дает результатов, территорию разбивают на полосы или квадраты и проводят сплошное обследование, при этом расстояния между точками погружения щупа определяются размерами и формой отыскиваемого предмета. Момент его обнаружения устанавливается по изменению плотности проверяемой среды, по упору в преграду. После извлечения щупа его поверхность осматривают в лупу, так как на ней могут быть наложения органо-тканевых частиц, волокнистых и других материалов.

Для проверки факта вскапывания грунта в ряде случаев целесообразно произвести отбор проб почвы. С этой целью щуп удлинительным стержнем и конусом

погружают в грунт на глубину 20–25 см, затем щуп извлекают и заменяют конус пробоотборной цилиндрической насадкой с боковой прорезью. Повторно вводят штангу с насадкой в грунт и углубляют ее на 10 см, после чего вытаскивают насадку, осматривают содержимое цилиндра и извлекают его на чистый лист бумаги. Наличие в изъятой пробе листьев, травы, щепок, углей, бумаги и иных посторонних примесей позволяет выдвинуть версию о вскапывании грунта.

В оснащение ПКЛ включен ручной бур АМ-16, снабженный тремя сменными буровыми стаканами. Вращая рукоятку, бур погружают в грунт и через интервалы в 20 см извлекают, а затем осматривают пробу, заполняющую стакан.

В криминалистическом комплекте следователя имеется тонкий щуп в виде заостренной спицы (длина 35 см), он используется для поиска предметов, спрятанных в мягкой мебели, подушках, матрацах, в мешках с сыпучими материалами и т. п.

Для поиска объектов на дне водоемов применяются тралы. Трал представляет собой металлическую рамочную конструкцию с захватными крючками и грузилом. У специалистов имеются тралы разной конфигурации с различной шириной захвата. Небольшой складной трал с набором запасных крючков и капроновым шнуром входит в комплект НТС прокурора-криминалиста. С помощью трала на дне водоема могут быть обнаружены труп и его части, одежда; предметы, упакованные в ткань, перевязанные веревками; пластиковые мешки и т. п. Поиск затонувших объектов с применением трала осуществляется путем его перемещения с лодки (траления) по предварительно намеченным параллельным полосам, ширина которых соответствует ширине захватной зоны трала. При зацепе за какой-либо предмет трал поднимают, осматривают предмет и крючки. В ходе следственных действий объекты, обнаруженные с помощью поисковых средств, извлекаются из воды, из мест укрытий, выкапываются из грунта в присутствии понятых с фиксацией факта обнаружения в протоколе.

Поисковые магнитные средства. В группу поисковых средств, основанных на использовании магнитных свойств, входят магнитные искатели и магнитометры.

Магнитные искатели (искатели — подъемники) — это постоянные магниты или системы магнитов различной формы и грузоподъемности, они предназначены для обнаружения объектов, притягивающихся к магниту. С помощью магнитных искателей удается отыскивать спрятанные или утерянные изделия из стали, чугуна, ферромагнитных сплавов, части и микрочастицы, относящиеся к таким изделиям (огнестрельное оружие, его детали, пули со стальной оболочкой и сердечником, орудия взлома, инструменты, крепежные элементы, а также опилки, стружку, обломки от стальных запирающих устройств, корпусов сейфов и т. п.). С помощью магнитных искателей могут быть найдены изделия из никеля (например, монеты), кобальта, частицы покрытия, отделившиеся от никелированного предмета. С учетом избирательного действия магнитных искателей не следует делать поспешных выводов об отсутствии искомого объекта при отрицательном результате: объект может быть изготовлен из немагнитного материала (например, нож из нержавеющей стали, не обладающий ферромагнитными свойствами; деталь из немагнитного чугуна). Магнитный искатель подковообразной формы с грузоподъемностью до 25 кг (при условии контакта обоих полюсов с объектом) входит в оснащение ПКЛ, к нему присоединяется шест иди капроновый шнур. Транспортируется искатель с замкнутыми якорем полюсами в стальном футляре. В переносном комплекте прокурора-криминалиста имеется подковообразный магнит с грузоподъемностью до 12 кг, он может использоваться в сочетании со штангой от щупа или со шнуром. Криминалистический комплект следователя включает искатель с магнитной го-

ловкой прямоугольной формы, шарнирно соединенной с хвостовиком, к которому присоединяется шнур или рукоятка с удлинительным стержнем от щупа. Подъемная сила магнитной головки при хорошей намагниченности достигает 8 кг.

Для поиска объектов на поверхности грунта, снежного покрова магнитный искатель присоединяется к штанге-рукоятке. Процесс поиска состоит в плавном перемещении магнита почти вплотную по намеченной полосе, ширина которой определяется длиной штанги. Необходимо обследовать каждое углубление, трещины почвы, при этом не следует поднимать магнит выше 1 см над поверхностью. При поиске объектов в песке, сухих листьях, мусоре, сугробах снега магнит вводят в обследуемую массу и перемещают в различных направлениях.

Поиск предметов в водоемах, колодцах, канализационных люках, ямах с нечистотами производится после проведения некоторых подготовительных операций. Перед началом работы магнит помещают в два вложенных один в другой полиэтиленовых мешка; под нижнюю поверхность магнита подкладывают прокладку из ткани, чтобы избежать повреждения пленки в момент притягивания предмета, и герметично перевязывают бечевкой мешки. Для улавливания момента обнаружения небольших предметов шнур присоединяют к динамометру и следят за изменениями его показаний. По завершении поиска, не снимая мешков, их ополаскивают вместе со шнуром, при необходимости дезинфицируют хлорамином, затем промывают струей воды, после чего снимают мешки с магнита.

При поиске микрочастиц, притягивающихся к магниту, в песке, пыли, на одежде, в карманах и т. п. в качестве поискового средства можно использовать магнитную кисть. Предварительно оттягивают хвостовик магнита и тщательно очищают изолирующий колпачок, затем проводят колпачком по местам возможного наличия частиц. Осторожно располагают «кисть» над листом чистой бумаги, оттягивают хвостовик — обнаруженные и изъятые микрочастицы падают на бумагу. Если необходимо обследовать на наличие микрочастиц поверхность большой площади (ковер, диван и т. п.), магнитный искатель заворачивают в целлофановую пленку, проводят по поверхности, после этого ставят магнит на чистый лист бумаги, разворачивают пленку, удаляют магнит, после встряхивания пленки частицы остаются на бумаге.

В щелях между досками, в углублениях, отверстиях микрочастицы можно обнаружить и извлечь намагниченным тонким щупом, спицей, препаровальной иглой (для намагничивания достаточно потереть конец инструмента об один полюс магнитного искателя).

Помимо искателей с одним магнитом в криминалистике применяются магнитные системы с несколькими магнитными элементами, грузоподъемная сила таких систем достигает 100 кг и более, расстояние захвата объектов повышается до 10–15 см. Поскольку многие системы имеют большой вес, их перемещают над обследуемой полосой на специальных тележках.

Для поиска предметов из ферромагнитных материалов в грунте, на его поверхности и в водоемах могут применяться магнитометры. Принцип действия этих приборов основан на индикации и регистрации изменения магнитного поля, вызванного объектами поиска. Имеется опыт применения ***магнитометра «Ferex 4.021 L» (Германия).*** Это прибор позволяет обнаруживать объекты на глубине до 6–7 м. Глубина обследования водоемов прибором ***«Ferex 4.021 W»*** достигает 20 м (максимальный вынос феррозонда прибора). Особенностью магнитометров является высокая точность определения местоположения и глубины залегания объекта. Координаты объекта могут быть определены в ходе поиска по показаниям прибора. При обсле-

дования больших территорий с засоренностью металлическими предметами производится запись сигналов на магнитном диске в процессе параллельных проходов, затем диск устанавливается в компьютер и по сигналам на мониторе определяются размеры и координаты объектов.

Химические поисковые средства. Группа химических поисковых средств охватывает приборы химического действия и специальные составы, используемые в процессе поиска объектов.

Для обнаружения находящихся в земле разложившихся трупов и их частей применяется трупоискатель — ***газоанализатор «Поиск-1».*** Прибор состоит из разборного трубчатого щупа, соединенного шлангом с ручным поршневым насосом, насос снабжен прозрачной индикаторной камерой. Внутри камеры расположены колбы с индикаторной текстильной лентой. Лента пропитывается реактивом следующего состава: уксуснокислый свинец — 2,4 г, подкисленная уксусной кислотой дистиллированная вода — 20 мл, глицерин — 3,5 г (для уменьшения испарения воды). Перед поиском территория разбивается на квадраты, в различных точках погружают щуп на разную глубину (предусмотрен передвигаемый ограничитель глубины) и производят отбор почвенного воздуха поршнем и последующим прокачиванием его через индикаторную ленту (пропускается 8–10 л почвенного воздуха). Если в воздухе почвы есть продукты гнилостного распада трупа — сероводород и меркаптаны, на индикаторной ленте в зоне штуцера появится желтое или коричневое пятно (при большом содержании продуктов распада — темный круг). Поскольку наблюдаемая реакция может указывать на трупы животных, необходимо произвести вскапывание и осмотреть извлеченные объекты с участием судебного медика. В зимнее время трупы замерзают и распад не происходит, поэтому применение прибора «Поиск-1» не дает результатов. Нельзя погружать щуп прибора ниже уровня грунтовых вод, в болотистую почву. Недостатками трупоискателя «Поиск-1» являются быстрое высыхание индикаторной ленты и недостаточно надежная индикация обнаружения объектов. Перспективным является сочетание газозаборного устройства с портативным газосигнализатором сероводорода со звуковой и световой индикацией. В некоторых моделях этих сигнализаторов применяется высокочувствительный керамический сенсор, действующий в течение двух лет без замены.

К приборам химического действия относится анализатор «Киноварь», применяемый для определения наличия ртути в воздушной пробе, а также обнаружения в багаже, ручной клади, почтовых отправлениях шлихового золота. Химическими поисковыми средствами являются различные составы (реактивы), используемые в целях обнаружения следов.

Для поиска и выявления невидимых и слабо видимых следов крови эффективным является применение раствора люминола. Кровь вызывает хемилюминесценцию щелочного раствора люминола в присутствии перекиси водорода — это выражается в голубоватом свечении, хорошо заметном в темноте. Свечение медленно угасает и возобновляется при добавлении новых порций раствора. Реакция с люминолом позволяет обнаруживать как свежую кровь, так и подвергнувшуюся гниению, атмосферным воздействиям, стирке, химической чистке, проглаживанию, смешиванию с водой. С помощью люминола можно установить наличие следов крови значительной давности (более года). Раствор люминола приготовляется следующим образом: в 1 л дистиллированной воды растворяются 5 г кальцинированной соды и 0,1 г люминола, непосредственно перед употреблением в раствор добавляется 100 мл трехпроцентной перекиси водорода (раствор после добавления перекиси водорода хранению не подлежит). Выявление следов проводится в затемненном помещении либо в тем-

ное время суток; применяются также затемнители в виде палаток. Раствор люминола наносят на поверхность с помощью пульверизатора, а при обработке большой площади — пневматическим распылителем. При появлении свечения обработку прекращают, осматривают объекты и изымают следоносители или следообразующее вещество. Необходимо иметь в виду, что хемилюминесценция наблюдается не только при взаимодействии раствора люминола с кровью, но и с некоторыми другими веществами (с жидким йодом, раствором перманганата калия, соком моркови, настоем чая, красным вином и др.), поэтому вопрос об образовании найденных следов кровью человека решается судебно-медицинской экспертизой. Применение раствора люминола не препятствует проведению в дальнейшем судебно-медицинских исследований по определению видовой и групповой принадлежности крови. Однако всегда желательно сохранение для экспертизы следов, пятен, участков на объектах, не подвергавшихся воздействию каких-либо реактивов.

Для проверки во время поиска следов возможности их образования кровью применяется также реактив Воскобойникова (основной или уксуснокислый бензидин — 1 г, лимонная или винная кислота — 10 г, перекись бария — 4 г; перед употреблением 0,1–0,2 г смеси растворяют в 10 мл воды), реактивом смачивают небольшой ватный тампон на стеклянной палочке или спичке, прикладывают тампон к краю следа, пятна. При появлении через 15–20 секунд на тампоне синей окраски можно считать, что образование следа (пятна) кровью не исключается. Работая с бензидиновыми реактивами, нужно соблюдать меры предосторожности, так как бензидин отнесен к канцерогенным веществам.

Удобным средством для определения наличия крови в следах и различных субстратах (смывах, внедрениях в текстильных тканях, в почве и т. д.) является индикаторная бумага «ГЕМОЦВЕТ-1», представляющая собой листы бумаги, на которые нанесен стабилизированный реактив азопирам. Бумагу смачивают 3 %-ной перекисью водорода и прижимают к следу; появление в течение до 2 минут в зоне контакта фиолетового окрашивания, переходящего затем в пурпурное, свидетельствует о возможном наличии крови.

При использовании реагента «ГЕМОФАН» достаточно увлажненную водой полоску наложить на край пятна — окрашивание в синий цвет считается положительной реакцией на возможное присутствие крови.

В целях обнаружения следов спермы используется специальный реагент «ФОСФО-ТЕСТ». Слой подложки индикатора, пропитанный указанным реагентом, прижимается к краю пятна (следа). Появление через 20–30 сек на подложке яркой фиолетовой окраски указывает на возможное наличие спермы. В протоколе следственного действия отражается факт применения реагента, появление окраски и локализация следа. Для решения вопроса о наличии на объекте спермы назначается судебно-медицинская экспертиза.

Поисковые технические средства химического действия применяются для обнаружения следов рук (нингидрин, аллоксан и др.). Специальные химические составы находят широкое применение в оперативно-розыскной деятельности для искусственного следообразования. Такие составы попадают на одежду, тело человека, их наносят на упаковки, денежные купюры, документы — все это помогает устанавливать незаконное проникновение преступника в помещение, контакты с определенными предметами, источники похищенных материалов и каналы их сбыта, дачу взятки и т. д. Состав используемых веществ включает базовые смеси с добавками (применительно к отдельным территориальным зонам). При попадании на объект некоторые спецсоставы вызывают появление яркоокрашенных трудносмываемых

следов; используются также вещества, люминесцирующие в ультрафиолетовых лучах, и составы с другими, доступными для обнаружения свойствами.

Поисковые средства электрического действия. В криминалистическом арсенале имеется небольшая группа поисковых средств электрического действия, в которую входят приборы, индуцирующие наличие или изменение параметров электрического тока, что используется для решения некоторых поисковых задач.

К данной группе относится сконструированный для криминалистических целей электрощуп. Прибор состоит из стальной штанги, на конце которой имеется конусный электродный наконечник с изолированными друг от друга электродами, соединенными с микроамперметром. Электрощуп может применяться для поиска закопанных и затопленных трупов и их частей на глубине до 1,4 м. С его помощью можно также отыскивать предметы, изготовленные из металлов, находящиеся в земле, воде, нечистотах, силосе и т. п., если контактированию наконечника с предметом не препятствует упаковка из диэлектрического материала. Действие прибора основано на индикации микроамперметром зоны пониженного удельного электросопротивления вокруг объекта органического происхождения (за счет растворения в воде продуктов гнилостного распада белковых веществ). Обнаружение металлических предметов происходит вследствие контакта их поверхности с электродами. В приборе предусмотрено ступенчатое изменение чувствительности в зависимости от электропроводности обследуемой среды.

К электрическим приборам, позволяющим обнаруживать наличие электрического напряжения на различных объектах, относятся индикаторы напряжения (ИО-500), ИН-01М и др.). Индикатор напряжения включен в криминалистический комплект следователя.

С применением индикаторов устанавливается наличие электрического напряжения в проводке, на корпусах распределительных щитов, деталях электрических приборов, на водопроводной арматуре, сантехнических устройствах и т. п. Применение индикатора, в частности, обязательно, когда оголенные провода или контактирующие с ними предметы препятствуют доступу к какому-либо объекту во время осмотра, обыска. Определив по свечению сигнальной лампочки наличие электрического напряжения, принимаются меры по обесточиванию проводки в помещении, при необходимости вызывают специалиста-электрика.

Во избежание поражения электрическим током запрещается пользоваться прибором, стоя на влажном грунте, бетонном полу, на мокрых досках без специальных средств защиты (диэлектрическая обувь, диэлектрический коврик, изолирующая подставка). Использовать индикатор можно для определения наличия напряжения не выше указанного на приборе предела. Если предполагается наличие более высокого напряжения, необходимые меры, обеспечивающие безопасность участников следственного действия, принимаются с привлечением соответствующего специалиста.

Индукционные поисковые средства. В группу поисковых средств, широко применяемых в криминалистической практике, входят индукционные металлоискатели. Поисковый элемент этих приборов в виде системы катушек формирует индукционное поле, параметры которого изменяются под воздействием искомого металлического предмета, что вызывает появление того или иного сигнала. Достоинством приборов индукционного типа является возможность применения их для отыскания объектов из черных и цветных металлов (в том числе драгоценных — золота, серебра, платины). Недостаток этих приборов — ограниченная чувствительность (максимальное расстояние от поискового элемента до объекта, на котором он может быть обнаружен). Чувствительность зависит от массы, размеров

искомого объекта, металла, из которого он изготовлен, а также от свойств окружающей среды, выполненной настройки — все это необходимо учитывать при использовании индукционных приборов.

В правоохранительных органах в течение многих лет применяется в качестве поискового технического средства ***миноискатель ИМП*** (индукционный миноискатель полупроводниковый). Поисковый элемент прибора, заключенный в герметичный пластмассовый кожух (это позволяет осуществлять поиск в воде), шарнирно закреплен на держателе разборной штанги и соединен кабелем с электронным блоком, снабженным головными телефонами. Настройка прибора выполняется двумя регуляторами: при отсутствии в радиусе 1,5 м металлических объектов поисковый элемент поднимают над землей на 10–12 см и вращают регуляторы до исчезновения основного тона в телефонах. Ориентировочная чувствительность прибора ИМП характеризуется следующими данными: пистолет Макарова (ПМ) может быть обнаружен на расстоянии 30 см от поискового элемента, пуля к этому пистолету (6 г) — на расстоянии 7 см, золотое кольцо (5 г) — на расстоянии 5 см.

Более широкими функциями обладает ***индукционный селективный металлоискатель «ИРИС».*** Прибор укомплектован двумя поисковыми датчиками: вытянутой формы — для поиска в помещениях и при личном обыске, круглой формы — в основном для поиска на местности. Прибор имеет автоматическую систему подстройки, звуковую, световую и стрелочную индикацию. В приборе «ИРИС» предусмотрены три режима поиска, каждый из которых избирается в зависимости от массы и размеров отыскиваемого объекта — это позволяет устранять помехи от посторонних мелких предметов (гвоздей, пробок от бутылок, кусков проволоки и т. п.), не интересующих следствие. В режиме «Поиск-1» чувствительность прибора с круглым датчиком позволяет обнаружить пистолет ПМ на расстоянии 40 см, пулю (6 г) — 10 см, золотое кольцо (5 г) — 10 см. В режиме «Сетема» имеется возможность определять параметры обнаруженного предмета (по соответствующему эквиваленту), а также глубину его залегания.

Также используется ***металлоискатель «СХ-Ц» фирмы «Гаррет» (США).*** Этот металлоискатель укомплектован четырьмя поисковыми элементами (для поиска на широкой ровной поверхности, точной локализации объекта, для поиска в кустах; универсальный датчик), кроме того, имеется приставка с двумя прямоугольными датчиками, расположенными во взаимно перпендикулярных плоскостях, что помогает обследовать большие горизонтальные поверхности (грунт, пол, перекрытия и т. п.) и вертикальные плоскости (обрывистые склоны, стены, ограждения и т. п.). Прибор имеет звуковую и стрелочную индикацию.

В режиме «Все металлы» прибор «СХ-П» обнаруживает черные и цветные металлы в пределах чувствительности, которая с поисковым элементом диаметром 30 см выше чувствительности прибора «ИРИС» примерно в полтора раза. Функция «Глубина» дает возможность определять глубину залегания объекта по шкале индикатора. В режиме «Разделение» (сетема) предусмотрено устранение регуляторами помех от мелких предметов из черных и цветных металлов (проволоки, фольги, монет и т. п.). По шкале индикатора возможна вероятностная дифференциация металлов: железо, золото, серебро — однако, как показала практика, не исключены и ошибочные показания. Звуковому сигналу можно придать различную тональность в зависимости от массы обнаруживаемого предмета. Металлоискатель «СХ-11» содержит управляющий микропроцессор, поддерживающий настройку, однако нужно учитывать, что при отсутствии в блоке питания батарей (аккумулятора) более 4 минут, установка звукового порога и чувствительности сбрасывается.

Модель металлоискателя «СХ-111» той же фирмы имеет «память», в которую можно внести задания на поиск предмета с определенными характеристиками (размер, вес, металл).

В органах МВД используются и другие индукционные металлоискатели со сменными поисковыми элементами, например, ***прибор «Бета» (ВМ-30Н***).

Вышеуказанные металлоискатели, снабженные штангами, могут применяться для поиска объектов на местности, в помещении, при проверке отдельных предметов. Перед началом работы приборы подлежат настройке по инструкции (при отсутствии системы автонастройки) и контрольной проверке путем приближения поискового элемента к эталону или другому металлическому предмету. На местности проводится выборочный и сплошной поиск. В последнем варианте территорию разбивают на полосы и медленно дугообразно перемешают поисковый элемент над поверхностью, не удаляя его более чем на 3 см. При появлении сигнала объект выкапывают, а если предполагается, что он взрывоопасный, отмечается его местонахождение и вызываются специалисты. Для проверки водоемов глубиной до 1 м могут применяться приборы ИМП и «ИРИС».

Металлоискатели индукционного типа часто используются в сочетании с механическими и магнитными поисковыми средствами (к прибору ИМП прилагается механический щуп).

Для поиска металлических предметов в помещениях и при личном обыске, помимо рассмотренных приборов, используются портативные индукционные металлоискатели. Очень простым прибором является ***металлоискатель «Гамма» (ВМ-20Н);*** пистолет ПМ обнаруживается им на расстоянии 14 см, пуля (6 г) — 7 см, золотое кольцо (5 г) — 6 см. Прибор настраивается одной ручкой на порог звукового сигнала. Удобными являются также малогабаритные приборы ***«ВМ-12Н», «Марс».***

В помещениях индукционные металлоискатели применяются для обнаружения тайников с металлическими предметами, спрятанного оружия, ювелирных изделий, золотых монет, металлических упаковок и т. д. При проверке стен помещений следует принимать во внимание наличие в них арматуры, балок, труб, электропроводки. После появления сигнала необходимо выявить другие признаки тайника: наличие полости, определяемое простукиванием, сверлением; отличие штукатурки, окраски в этой зоне.

С помощью металлоискателей проверяются пакеты, стеклянные банки, мешки, деревянные бочки, ящики, коробки — на наличие металлических вложений, а также предметы мебели, в которых могут быть небольшие тайники со спрятанным оружием и т. п. Естественно, мягкую мебель с металлическими сетками, пружинами проверяют не металлоискателем, а другими средствами, в частности, тонким щупом.

В оперативно-розыскной деятельности органов МВД применяется ***металлоискатель «Колос»,*** предназначенный для обнаружения переносимого огнестрельного и холодного оружия (обнаружение пистолета ПМ на расстоянии 20 см, охотничьего ножа — 17 см); прибор незаметно размещается под одеждой оперативного работника.

Поисковые средства излучающего действия. Большим разнообразием отличаются поисковые средства излучающего действия. К этой группе средств относятся универсальные фонари с регулируемым рефлектором, светорассеивающими насадками, зеркалами и лупами, позволяющие создавать различные варианты освещения (косопадающее, перпендикулярное, бестеневое), необходимое для обнаружения предметов, следов и микрочастиц на ровных или неровных поверхностях. Для выявления окрашенных (хроматических) следов и частиц в сочетании с фонарями применяются светофильтры.

К поисковым приборам излучающего действия относится ***портативный детектор скрытых следов преступлений (ПДСП);*** в этом приборе источником излучения является лазер типа «ЛАЗЕКС», наблюдение вызываемой им люминесценции следов рук и других объектов ведут через специальные очки со светофильтрами.

Своеобразными средствами для визуального поиска объектов в труднодоступных местах, в багаже без его распаковки, в автомобилях являются гибкие и полужесткие эндоскопы (ТЭГ, ТЭП), в которых освещение и наблюдение осуществляется с помощью светопроводящих гибких жгутов.

В практической деятельности правоохранительных органов важную роль играют ультрафиолетовые осветители (излучатели), их применение эффективно для обнаружения объектов, люминесцирующих в ультрафиолетовых лучах (горюче-смазочные материалы, капли ружейной смазки, химические отбеленные натуральные волокна, спецсоставы, некоторые синтетические краски, следы кислот и щелочей, стиральные порошки, следы спермы и др.). Следы крови (без обработки) в ультрафиолетовых лучах не люминесцируют, они остаются темно-коричневыми, но могут стать заметными на люминесцирующем фоне. Биологические следы не следует облучать более 5 сек., так как это может разрушить молекулы ДНК. Криминалистами много лет успешно используется ультрафиолетовый осветитель УК-1 с аккумуляторным питанием. Более поздними моделями являются осветитель УО-1 (может использоваться и как фонарь), портативные осветители «Таир-1», «Квадрат». В стационарных условиях применяются осветитель ОЛД-41, криминалистический вариант осветителя «Фотон» и другие приборы.

Для обнаружения на темном фоне следов темных веществ и микрочастиц (следы сажи, копоть, резина, частицы пороха, поясок обтирания, уголь и т. п.), а также для выявления некоторых подделок в документах (дописки, исправления, карандашная подготовка) и обнаружения залитых, замазанных текстов (знаков) прибегают к использованию инфракрасных излучений в сочетании с электронно-оптическими преобразователями. Источником инфракрасных лучей обычно служит лампа накаливания, наблюдение ведут через электронно-оптический преобразователь (ЭОП), снабженный инфракрасным светофильтром (приборы С-ЗЗО, инфракрасный монокуляр ЛИ-1) «Эдельвейс» с удлинительным кольцом и др.). В оперативно-розыскной деятельности в инфракрасных лучах осуществляют ночной поиск прячущихся лиц, ведут наблюдение при низкой освещенности (применяются приборы «Ворон-3», «Эдельвейс», «Филин» и др.).

Для решения задач поиска привлекаются приборы с проникающими излучениями. К использованию этих приборов прибегают, когда необходимо проверить внутреннее содержание объектов без нарушения целостности их корпуса, оболочки, конструкций, без вскрытия упаковок, с исключением каких-либо манипуляций ручками управления и т. п. В частности, необходимость в интроскопическом обследовании проникающими излучениями (с участием специалиста) возникает, когда есть основания считать объекты взрывоопасными. Попытки вскрытия таких объектов (почтового отправления, чемодана и т. п.), нажатие кнопок включения «фонарика», «диктофона», «электробритвы» и т. п. может привести к тяжелым последствиям.

Для «просвечивания» стен, сейфов, металлических конструкций, багажа в целях обнаружения оружия и боеприпасов, взрывных устройств, тайников, радиозакладок — при проведении осмотров и обысков предназначена рентгенотелевизионная установка типа «Заслон». Обследование малоформатных объектов (небольшой плотности) может быть осуществлено переносной рентгеновизуальной установкой

«Гортензия-Т», а также переносными ***флюороскопами ФП-1, ФП-2, ФП-4***. В экспертных лабораториях органов МВД имеются стационарные рентгеновские аппараты. При подозрении на проглатывание человеком небольших предметов (например, ювелирных изделий) рентгеновское исследование может проводиться только врачом-рентгенологом; в дальнейшем субъект направляется в медицинское учреждение для необходимых процедур.

Помимо рентгеновской аппаратуры в криминалистических целях используются проникающие радиоактивные излучения. Проверка малогабаритных упаковок, содержимого пакетов, банок, выявление тайников может быть выполнено с помощью портативного изотопного флюороскопа ФП-3.

В органах МВД имеется ***радиометрический прибор «Олива-М»,*** который позволяет обнаруживать небольшие предметы из золота на расстоянии до 25 см, в том числе расположенные за стальным листом толщиной до 2 мм (например, в багажнике автомобиля).

При необходимости в процессе расследования провести интроскопическое обследование крупногабаритных объектов (контейнеров, цистерн, сейфов, перекрытий, стен) следователь может обратиться за технической помощью в строительно-монтажные учреждения, где имеются выездные изотопные дефектоскопические лаборатории, ультразвуковые томографы и другая аппаратура.

Во всех случаях обслуживание поисковых средств с вредными проникающими излучениями должно осуществляться специалистами, имеющими допуск к работе с соответствующей аппаратурой, при этом соблюдаются правила, обеспечивающие полную безопасность всех участников следственного или оперативного мероприятия и окружающих.

В отличие от приборов с активным излучением действие ряда поисковых средств связано с восприятием излучений (информационных сигналов), свидетельствующих о наличии искомого объекта.

§ 2. Средства поисковой техники

Средства поисковой техники применяются для обнаружения вещественных доказательств и предметов, которые предположительно могут стать вещественными доказательствами или способствовать установлению новых фактов преступной деятельности, содействовать выбору тактических приемов проведения следственных действий и уточнению методических схем расследования. Применение поисковых приборов позволяет значительно сократить время обнаружения представляющих интерес предметов и объектов.

Принцип работы поисковой техники основан на обнаружении объектов, по каким-либо физическим параметрам отличающихся от параметров укрывающей их среды. В качестве объектов, которые обнаруживаются поисковыми приборами, могут выступать тайники в различных средах, наркотические и взрывчатые вещества, изделия из черных и цветных металлов, скрытые письменные знаки, различные следы биологического происхождения. Широкий набор поисковых средств вызван достаточно большим разнообразием предметов, представляющих интерес, а также видов укрывающих сред (эти предметы могут быть спрятаны в земле, воде, в стенах зданий, вещах, мебели и т. д.).

Принято выделять три группы поисковых приборов: контактные, неконтактные и вспомогательные.

Контактные поисковые приборы работают на принципе непосредственного механического контакта с искомыми предметами и укрывающей средой. К ним относятся магнитные искатели-подъемники, представляющие собой мощный постоянный магнит, а также буры, кошки, тралы, щупы.

Неконтактные приборы обнаруживают искомый объект с некоторого расстояния без непосредственного контакта с ним. В основу действия этих приборов положены разнообразные физические явления, а поиск предметов осуществляется благодаря наличию вторичных признаков искомых предметов. При этом используются химические методы экспресс-анализа веществ и проб воздуха, радиоактивное и рентгеновское излучения, вихревые токи, явления взаимоиндукции и др.

К приборам этой группы относятся приборы для поиска изделий из черных и цветных металлов, пустот и неоднородностей, рентгеновские установки, приборы для поиска и идентификации взрывчатых и наркотических веществ.

Поисковые приборы, относящиеся к группе **вспомогательных,** позволяют исследовать предметы в инфракрасных и ультрафиолетовых лучах. Приборы, использующие инфракрасное излучение, действуют по принципу преобразования инфракрасного излучения из невидимого в видимый участок спектра. Они используют свойства некоторых объектов, не прозрачных при обычном освещении, быть прозрачными в инфракрасных лучах. При исследовании в инфракрасных лучах можно обнаружить скрытые изменения текста (подчистки, травления), следы обводки, залитые тексты, если красители текста и заливки отличаются по плотности, и другие.

Приборы исследования в ультрафиолетовых лучах, ультрафиолетовые осветители, предназначены для возбуждения люминесценции веществ. Известно, что большое количество веществ люминесцируют в ультрафиолетовых лучах (светятся различными цветами). В связи с этим, наличие даже небольшого количества такого вещества на предмете, не видимое в обычных условиях, проявится при ультрафиолетовом освещении. По изменению характера люминесценции (цвета и интенсивности) можно определить несоответствие по времени нахождения этого вещества на каком-либо предмете. Кроме этого, приборы такого типа используются для исследования денежных купюр и документов, имеющих люминесцентную защиту.

Среди приборов для поиска изделий из черных и цветных металлов наиболее распространенными являются металлоискатели, предназначенные для отыскания металлических предметов и изделий. В основу действия разработанных в последнее время конструкций металлоискателей заложен принцип регистрации поля вихревых токов, наводимых в металлических предметах под воздействием излучаемых прибором электромагнитных импульсов.

Металлоискатель «Марс» предназначен для поиска металлических изделий в одежде, носимых вещах и иных мелких предметах. Прибор реагирует на обнаружение металла звуковой индикацией. Максимальное расстояние обнаружения для предметов размерами $100 \times 100 \times 1$ мм составляет 120 мм. Прибор прост в эксплуатации, не требует настройки.

АК-7215 «Уникан» может быть использован как для обследования небольших предметов, так и для поиска металлических изделий в грунте, снеге, багаже. Он имеет звуковую и световую индикацию обнаружения. При обнаружении предмета из черного металла прибор выдает монотонный звуковой сигнал, а при наличии цветного металла звуковой сигнал носит прерывистый характер (соловьиная трель). Перед применением прибор необходимо настроить. Имеется дополнительный режим работы, в котором прибор не реагирует на цветные металлы. Особенностью прибора является то, что он обнаруживает металл только в динамике, т. е.

при перемещении искомого объекта относительно поискового элемента. Максимальная глубина обнаружения металлических изделий составляет 80 см (люк колодца). Пистолет Макарова обнаруживается с расстояния 35 см.

Прибор «Ирис-Э» может использоваться преимущественно для обследования участков местности. В комплект входят два типа поисковых элементов различного размера и конфигурации. Один из них предназначен для обнаружения крупных объектов, расположенных на большом расстоянии, другой — для поиска мелких предметов, находящихся на незначительном удалении. Прибор имеет три типа индикации: стрелочную, звуковую и световую.

Прибор имеет три режима поиска, каждый из которых отличается наибольшей чувствительностью к предметам с соответствующими размерами и массой.

Дополнительно данный металлоискатель имеет режим определения эквивалентной электропроводящей массы обнаруженного предмета (под этой характеристикой понимают комплексный параметр, зависящий от геометрических размеров, массы металлических предметов, их электромагнитных характеристик).

Подводный металлоискатель «Ирис-П» предназначен для работы под водой в пресных и соленых водоемах при любой прозрачности воды на глубинах до 40 м. Прибор имеет оптическую индикацию о наличии объекта поиска и направлении на него, разряде источника питания.

Селективный металлоискатель «Кедр» имеет стрелочную и звуковую индикацию результатов поиска. При обнаружении черных металлов раздается звук высокого тона, а цветных — низкого.

Для избирательного обнаружения золота служит отдельная группа поисковых средств, называемая золотоискателями.

Прибор «Киноварь» обнаруживает золото по косвенному признаку — наличию паров ртути в окружающем воздухе, так как ртуть используется как один из компонентов технологического процесса механизированной добычи золота. Он используется для определения такого золота в одежде, ручной клади, почтовых отправлениях и др.

Прибор работает следующим образом. На первом этапе пробы воздуха прокачиваются через сорбент, который накапливает находящуюся в воздухе ртуть. Затем производится процесс отжига сорбента. Ртуть уже значительно большей концентрации начинает проходить через кювету, где подвергается монохромному облучению, генерирующемуся высокочастотной спектральной лампой. Часть этого излучения поглощается парами ртути, а разница энергий падающего и прошедшего через кювету излучения регистрируется и служит основой для измерения концентрации паров ртути в кювете. Количество паров ртути отображается на цифровом табло прибора.

Процесс работы и конструкция допускает отборы проб воздуха с помощью сорбента отдельно от остальных частей прибора, что позволяет производить измерения в труднодоступных и удаленных местах.

Приборы для поиска пустот и неоднородностей предназначены для обнаружения тайников и вложений. ***Прибор «Кайма»*** обеспечивает поиск воздушных полостей в кирпичных и бетонных стенах и перекрытиях. Его принцип действия основывается на свойстве электромагнитных волн частично отражаться от границ раздела двух сред различной плотности. Отраженный сигнал, представляющий собой часть излученной прибором волны, обрабатывается и поступает на стрелочный и звуковой индикатор. Дальность обнаружения пустот зависит от их размера и составляет от 60 до 250 мм, на показания прибора не влияет то, что полость может быть заполнена различными вложениями.

Прибор «Жасмин» предназначен для обнаружения габаритных тайников, расположенных в грунте, кирпичных и бетонных стенах на больших глубинах. В приборе используется импульсное излучение. Обнаружение неоднородности осуществляется по времени задержки прихода отраженного сигнала. Максимальная глубина обнаружения составляет 50 см для пустот, расположенных в глинистых и песчаных грунтах. В кирпичных стенах прибором можно обнаружить полости на глубине до 50 см, в бетонных — 20 см. В комплект дополнительно входит устройство для сверления и эндоскоп для осмотра содержимого полости через просверленное отверстие.

Принцип работы ***рентгеновской установки «Гортензия-0» (АРС-1)*** основывается на способности рентгеновского излучения проникать через различные предметы. Рентгеновское излучение, формируемое установкой, проходит через контролируемый объект и преобразуется в видимое изображение на специальном экране. В результате на экране в виде темных и светлых объектов будет отображаться структура обследуемого предмета.

Рентгеновская установка предназначена для обнаружения диэлектрических и металлических вложений в одежде и других мелких предметах. Установкой могут быть обнаружены денежные купюры и записки, различные наркотические и лекарственные вещества в виде таблеток и порошков, а также практически любые иные, в том числе и металлические, предметы. Важно, чтобы способность к поглощению рентгеновского излучения укрывающей среды была меньше, нежели степень поглощения искомого предмета.

Приборы для поиска и идентификации взрывчатых веществ представляют собой газоанализаторы, регистрирующие наличие паров взрывчатых веществ в отобранной пробе воздуха. ***Газоанализатор «Шельф»*** имеет пороговую чувствительность не хуже 10 г/см, время отклика составляет 1–2 секунды.

Для поиска взрывчатых веществ предназначен и ***газовый хроматограф «Эхо-М»*** — носимый автономный газоанализатор с сорбированием пробы воздуха. Определение наличия вещества в пробе осуществляется с помощью газохроматического анализа. Прибор работает под управлением встроенной микро-ЭВМ, существует возможность связи с персональным компьютером.

Приборы «Сверчок» и «Репер-3» функционируют на принципе регистрации отражения нейтронного излучения от исследуемых веществ. Так как атомы водорода имеют особый характер отражения нейтронов, то по отраженному потоку можно судить о присутствии водородосодержащих веществ, например, взрывчатых или наркотических. Основное назначение приборов — обнаружение веществ за обшивкой и в полостях транспортных средств. Прибор «Сверчок» регистрирует минимальную массу водородосодержащего вещества 50 г, находящегося за стальной обшивкой толщиной 3 мм на глубине до 50 мм. Прибор «Репер-3» обнаруживает минимальную массу 450 г на глубине до 65 мм.

Недостаток данных приборов заключается в регистрации не только взрывчатых или наркотических веществ, но и других водородосодержащих веществ, таких как мыло, бумага и т. д.

Среди индикаторов наркотических веществ следует отметить комплект ***«Наркотест».*** Он представляет собой набор ампул с реагентами на определенные виды наркотических веществ и фармацевтических препаратов. По окрашиванию результатов химических реакций можно судить о наличии наркотика в исследуемом веществе. «Наркотест» обеспечивает быстрое выявление и предварительную идентификацию практически всех наркотических средств.

Несколько особое место в группе поисковых приборов занимает прибор «***Контраст-М»,*** предназначенный для оперативного выявления признаков модификации маркировочных данных на кузовах автотранспорта. Он может регистрировать вварку, напайку, наклейку металлических пластин и фрагментов с фиктивными маркировочными данными, изменение толщины лакокрасочного покрытия в зоне маркировки и др. Прибор имеет звуковую, световую и стрелочную индикацию обнаруженных дефектов.

§ 3. Магнитометрические средства обнаружения

Магнитометрические средства обнаружения (МСО) предназначены для регистрации факта проноса в их чувствительной зоне предметов, выполненных из металлов или их сплавов.

МСО различают по физическим принципам действия, заложенным в основу построения средств обнаружения, как то:

- с использованием эффекта переизлучения сигнала;
- с использованием эффекта биения частоты;
- с использованием эффекта самоиндукции;
- с использованием эффекта локального искажения магнитного поля Земли.

Рассмотрим кратко физическую суть изложенных принципов.

Средство обнаружения с использованием эффекта переизлучения сигнала (СОП) содержит две катушки — передающую и приемную. На передающую катушку подается опорный сигнал, частота и амплитуда которого постоянны во времени. Посредством передающей катушки этот сигнал излучается в окружающую среду. За счет явления самоиндукции во встреченном на пути сигнала проводящем предмете наводится ЭДС, которая в свою очередь вызывает излучение этим предметом «вторичного» поля, т. е. имеет место переизлучение сигнала.

Переизлученный сигнал принимается приемной катушкой СОП. Для ослабления эффекта прямого наведения ЭДС на приемную катушку от передающей, катушки располагают под углом друг к другу или даже разносят в пространстве.

Данное МСО обладает селективностью — четко выраженной способностью различать объекты, изготовленные из различных металлов и сплавов, по фазе отраженного сигнала за счет оптимизации выбора частоты сигнала излучающей катушки.

Уровень сигнала, наводимого в приемной катушке, обратно пропорционален 6–7-й степени расстояния до обнаруженного предмета. СОП имеет четко выраженную диаграмму направленности. За счет этого он теоретически обладает максимальной помехоустойчивостью по сравнению с другими типами средств обнаружения аналогичного назначения.

Схема применяется в подавляющем большинстве зарубежных средств обнаружения. Обладает свойством обнаруживать объекты с минимальными размерами по сравнению с другими СО.

Средство обнаружения с использованием эффекта переизлучения сигнала, содержащее одну катушку индуктивности для передачи и приема сигналов (СОИН), содержит только одну катушку индуктивности, возбуждаемую переменным током. При приближении катушки к металлическому предмету появляется переизлученный сигнал, который наводит в ней дополнительную ЭДС.

Уровень сигнала, наводимого в катушке, обратно пропорционален 6-й степени расстояния до обнаруженного предмета. СОИН сочетают в себе чувствительность

и селективность к металлам СОП и простоту конструкции СОБ, который будет рассмотрен ниже. Недостаток — необходимость компенсации изменения параметров катушки индуктивности от температуры, так как в принципе действия СОИН заложено не только реагирование на полезный отраженный сигнал, но и на любое изменение параметров чувствительного элемента.

Средство обнаружения с использованием эффекта биения частоты (СОБ) содержит два генератора, частоты которых при отсутствии внешних дестабилизирующих факторов равны.

Генераторы отличаются друг от друга тем, что частота первого стабильна и не зависит от внешних дестабилизирующих факторов, а частота второго может меняться.

Частоты генераторов поступают на устройство сравнения, выделяющее разностную частоту. Сигнал на выходе устройства появляется только в случае неравенства частот и он тем выше, чем больше это неравенство.

Изменение частоты второго генератора происходит за счет изменения параметров колебательного контура, определяющего частоту настройки генератора. Индуктивность колебательного контура может меняться за счет приближения последнего к металлическому предмету.

Таким образом, при отсутствии металла частоты генераторов равны и разностный сигнал равен нулю. Наличие металла приводит к перестройке контура нестабильного по частоте генератора и появлению разностного сигнала.

Уровень разностного сигнала обратно пропорционален 6-й степени расстояния от обнаруженного предмета. По сравнению с другими типами магнитометрических средств обнаружения, СОБ обладает малой дальностью обнаружения вследствие эффекта паразитной синхронизации. Сетема по металлам отсутствует.

Рассмотренный принцип действия средств обнаружения широко использовался в первых промышленных моделях миноискателей.

Средство обнаружения с использованием эффекта самоиндукции (СОИМ). Принцип действия СОИМ похож на СОП. Отличие заключается в том, что в СОП сигнал излучается и принимается непрерывно, например, в виде импульсной последовательности, а в СОИМ — в виде одиночных импульсов. В состав СОИМ обычно входят генератор импульсов тока, приемная и излучающая катушки, устройство коммутации и блок обработки сигналов.

Уровень сигнала, наводимого в приемной катушке, обратно пропорционален 4...6-й степени расстояния до обнаруженного предмета. Практически отсутствует сетема по металлам. Существенный недостаток СОИМ в том, что он является источником помех импульсного характера.

Средство обнаружения с использованием эффекта локального искажения магнитного поля Земли (СОМ). Принцип действия этого вида средства обнаружения основан на явлении локального искажения магнитного поля Земли ферромагнитными материалами. Он обладает максимальной дальностью обнаружения. Это объясняется тем, что аналогом излучаемого поля для магнитометров является сильное однородное магнитное поле Земли, поэтому отклик на ферромагнитный предмет обратно пропорционален 3-й степени расстояния. К недостаткам СОМ, как правило, следует отнести большие габаритные размеры и массу, а также невозможность обнаружения предметов из цветных металлов.

Условно все МСО можно разделить на пассивные и активные. На практике в оперативных мероприятиях стараются применять пассивные МСО, т. е. такие, собственное излучение у которых отсутствует. Пассивные МСО значительно труд-

нее обнаружить, а значит легче камуфлировать. Активные МСО применяют в тех случаях, когда не требуется их камуфлировать по излучению.

К активным магнитометрическим средствам обнаружения можно отнести СОП, СОБ, СОИН и СОИМ, к пассивным — СОМ.

Главное назначение МСО — поиск оружия. Поэтому к основным характеристикам МСО можно отнести дальность обнаружения металлических предметов и помехоустойчивость.

Наибольшую дальность обнаружения имеет пассивное средство СОМ, а наиболее помехоустойчивым является активное средство СОП. В то же время СОП позволяет определить вид металла, из которого изготовлен обнаруженный предмет.

На практике СОМ часто используется в камуфлируемой аппаратуре для обнаружения оружия. Такая аппаратура устанавливается скрытно и может работать длительное время в автономном режиме, так как собственное потребление СОМ незначительно или отсутствует. Благодаря пассивному характеру работы СОМ обнаружить такую аппаратуру по собственному излучению очень трудно. Наиболее важной характеристикой СОМ в этом случае является именно дальность обнаружения, так как специальные методы обработки сигналов позволяют существенно скомпенсировать чувствительность устройства к помехам.

Наиболее характерная область применения СОП — миноискатели. В этой аппаратуре идеально сочетаются сравнительно малые массогабаритные характеристики СОП с его высокой помехоустойчивостью. Дальность обнаружения не имеет существенного значения, так как мины часто устанавливают на малой глубине. Собственное излучение СОП в данном случае значения не имеет.

Важнейший параметр огнестрельного оружия, влияющий на уровень полезного сигнала как активных, так и пассивных МСО, — остаточная намагниченность оружия. В то же время остаточная намагниченность оружия — это единственный параметр, определяющий уровень полезного сигнала пассивных МСО. Характерными местами расположения магнитных масс огнестрельного оружия являются область дула и, как правило, диаметрально противоположная ей область — до 50 %. Однако уровень полезного сигнала существенно зависит и от амплитуды колебания оружия при его переноске. В качестве примера можно привести увеличение уровня полезного сигнала от автомата Калашникова примерно в 3...5 раз при его проносе мимо МСО с амплитудой колебания его дула примерно на 0,1 м с частотой около 1 Гц.

В подавляющем большинстве случаев средства обнаружения применяют для негласного контроля за пересечением вооруженными людьми контролируемой зоны.

Как было сказано ранее, магнитометрические средства обнаружения применяют для выявления факта проноса на охраняемую территорию предметов с магнитными свойствами. В основу построения МСО могут быть положены три группы методов:

- с использованием феррозондов;
- с использованием пассивных катушек;
- квантовые измерители индукции.

Феррозондом называется устройство, чувствительное к внешним магнитным полям, главным образом постоянным и медленно изменяющимся, содержащее ферромагнитные сердечники и обмотки, распределенные по их длине.

От пассивных индукционных датчиков и ферритовых антенн феррозонды отличаются тем, что являются устройствами активного типа. Происходящие в них процессы всегда связаны с существованием двух полей — внешнего измеряемого поля и некоторого вспомогательного поля, образуемого за счет тока, протекающего в одной из его обмоток. Взаимодействие этих полей в объеме сердечников, изготав-

ливаемых из легко насыщающихся магнитных материалов, например, пермаллоя, приводит к появлению в другой обмотке электродвижущей силы, по величине которой и судят о напряженности внешнего поля.

Существует довольно много типов и модификаций феррозондов. Все они отличаются друг от друга режимом работы, способом наложения вспомогательного поля, выбранной схемой и конструктивным исполнением. Эти отличия оказываются более или менее существенными в зависимости от диапазона и частотного спектра измеряемых полей, условий, в которых проводятся измерения, особенностей преобразования полезного сигнала в измерительной схеме. Однако феррозондам присущи и некоторые общие свойства.

§ 4. Технические средства поиска наркотических веществ

Поиск и обнаружение наркотических веществ, как составляющая оперативной задачи поиска и обнаружения предметов контрабанды, в настоящее время приобрела особую актуальность. Все увеличивающийся объем потребления наркотических веществ в разных странах, а, следовательно, их перемещение через государственные границы, вступление нашей страны в международный Совет таможенного сотрудничества и вытекающие из этого обязательства потребовали от наших таможенных служб более целенаправленной организации работы по выявлению в перемещаемых через госграницу объектах наркотических веществ (НВ).

В мировой таможенной практике пока отсутствуют технические средства, позволяющие однозначно с высокой степенью достоверности обнаруживать НВ в любых видах контролируемых объектов и оперативных условиях, хотя отдельные попытки по их созданию в ряде передовых стран ведутся.

Для обнаружения НВ применяются технические средства контроля на базе приборных физических и физико-химических методов (рентгеноскопия, метод ядерно-квадрупольного резонанса, хромато-масс-спектрометрия, спектроскопия ионной подвижности) и метод с использованием специально подготовленных собак.

Рентгеноскопия основана на регистрации изменения интенсивности рентгеновского излучения после прохождения через досматриваемый объект и широко используется в промышленности и медицине. Установки для рентгеновского досмотра багажа фирмы RAPISCAN серии 500 — это передовая рентгеновская технология, в сочетании с уникальной обработкой изображения обеспечивает новый уровень качества изображения. Все модели оборудованы цветными мониторами SVGA 17" высокого разрешения, рентгеновские детекторы покрыты защитным слоем, в несколько раз увеличивающим их долговечность.

Компьютерная обработка изображения сканируемого объекта обеспечивает глубокое проникновение, высокую резкость и великолепную разрешающую способность.

Физические методы — рентгеноскопия предназначены для обнаружения сосредоточенных масс НВ и даже в лучших образцах имеют предел обнаружения НВ на уровне долей килограмма. Специфичность обнаружения НВ достаточно высокая, рентгеноскопия в широко распространенных моделях не специфична по отношению к НВ и позволяет только обнаруживать места сокрытия контрабанды с отличающимися от упаковки показателями поглощения рентгеновского излучения. Под специфичностью в данном контексте следует понимать параметр обратно пропорциональный частоте ложного срабатывания метода. Высокоспецифичные

методы имеют очень малое количество ложных срабатываний в процессе эксплуатации.

К недостаткам физических методов следует отнести экранирование сигнала металлической тарой (упаковкой) и, как следствие, невозможность обнаружения НВ в металлических контейнерах. Для непроводящей тары физические методы оптимальны и активно используются даже на конвейерных линиях.

Третье направление создания технических средств поиска НВ основано на свойстве наркотиков — их аэрозольной дисперсии, т. е. присутствии микрочастиц вещества в воздушной среде (в нашем случае — в упаковках НВ) и, следовательно, обладающих всеми характерными для своих видов физико-химическими параметрами. Выделение предельно малых количеств веществ из забираемой из подозрительной упаковки воздушной пробы и сравнение их характеристик с заложенными в банке данных ЭВМ параметрами известных НВ дает достаточно точный ответ на присутствие (или отсутствие) НВ в контролируемой упаковке или объеме.

Физико-химические методы обнаружения НВ (хроматографические и ионно-дрейфовые приборы, сенсорные датчики) определяют наличие НВ по летучим компонентам пробы. Для достижения высокой чувствительности обнаружения НВ в хроматографических и ионно-дрейфовых методиках требуется концентрирование пробы, поэтому достаточно большой объем воздуха просасывается через сорбционный преконцентратор. Преконцентратор помещается в термодесорбер и сконцентрированная проба вводится в аналитический тракт прибора. Хроматографические методы позволяют провести идентификацию НВ по индексу удерживания и, в случае масс-спектрального детектора, по ионным массам продуктов фрагментации НВ.

Следует отметить, что в процессе использования сорбционного преконцентратора происходит концентрирование не только целевого компонента (НВ), но и всех остальных органических примесей, содержащихся в анализируемом воздухе. Это обстоятельство способно значительно ухудшить как процесс хроматографического разделения, так и процесс идентификации НВ, ибо содержание в воздухе паров растворителей или горюче-смазочных материалов, как правило, значительно превышает содержание паров НВ. В этой связи реально достигаемую специфичность обнаружения и идентификации НВ в методиках, использующих преконцентратор, следует обязательно оценивать экспериментально.

Интересен также ***детектор контрабанды Sentinel,*** который представляет собой пропускной контур для прохождения людей, способный обнаружить до 30 различных видов взрывчатых, наркотических и токсичных соединений. Работа пропускного детектора полностью автоматизирована, и при срабатывании происходит подача звукового и светового сигнала.

Детектор Sentinel отличается высокой чувствительностью, селективностью и возможностью перенастройки с учетом конкретных задач. Детектирование происходит бесконтактным методом, что является необходимым для пропускания большого числа людей в аэропортах, на стадионах, общественных местах или в зоне таможенного контроля. Пропускная способность контура составляет 7 человек в минуту. Следовые количества химического оружия могут быть определены в зоне военных действий после проведения детоксикации личного состава и обмундирования. При доукомплектовании магнитометром Sentinel может срабатывать не только на наркотики и взрывчатку, но и на оружие и другие металлические предметы. Таким образом, Sentinel является идеальным детектором для обеспечения безопасности, выявления случаев контакта со взрывчаткой или наркотиков и задержания лиц, их распространяющих или передающих.

В связи с не абсолютной специфичностью методов обнаружения НВ все случаи положительного срабатывания или сомнительные нуждаются в процедуре идентификации НВ. Процедура идентификации может быть выполнена как в стационарных условиях экспертно-криминалистических лабораторий приборными методами ТСХ, ГЖХ, ВЭЖХ, хромато-масс и ИК-спектрометрии, так и в полевых условиях экспресс-методами на основе мокрой химии.

В настоящее время одним из наиболее совершенных комплектов для обнаружения наркотических средств и психотропных веществ является ***комплект «НАРКОЦВЕТ»,*** который предназначен для анализа твердых и жидких объектов, растительного материала. Принципиальным отличием комплекта от известных отечественных и зарубежных аналогов является то, что в нем впервые реализована схема цифровой кодировки окраски, образующейся в результате обработки исследуемого объекта и химического реактива.

Реализовать указанную схему удалось после создания целого ряда модифицированных химических реактивов, обладающих повышенной селективностью и чувствительностью. В результате удалось в значительной мере избавиться от ошибок, связанных с нарушениями в последовательности проведения тестирования, присущих комплектам других производителей. Кроме того, данная схема позволяет достаточно просто автоматизировать процесс считывания результатов. В настоящее время, по имеющейся информации, разработчиками комплекта проводятся работы по созданию автоматического счетчика результатов тестов.

В состав комплекта входят:

– тест НАРКОЦВЕТ-Б — для обнаружения барбитуратов, кокаина (гидрохлорида, основания), КРЭК, эфедрина, метаквалона, димедрола, амфетаминов различных групп, апрофена, циклодола, промедола, трамала, морфина, ЛСД, амизила, героина, кодеина и фенциклидина;

– тест НАРКОЦВЕТ-М1 — для обнаружения наркотических веществ в растительных материалах (солома мака, гашиш, марихуана, опий и его водные растворы, трава эфедры);

– тест НАРКОЦВЕТ-М2 — для обнаружения бупренорфинов.

Комплект НАРКОЦВЕТ обладает наибольшей селективностью по отношению к наркотическим и сильнодействующим веществам и отличается минимальными массо-габаритными параметрами (110 × 120 × 10 мм при массе не более 90 г). Ампулы помещены в пенал из прозрачного материала, и все реакции проводятся одновременно, что сокращает время проведения анализа до 2…4 минут. Существенно упрощена система идентификации наркотических и сильнодействующих веществ в исследуемой пробе. В зависимости от конкретных задач комплектация и состав теста может изменяться.

§ 5. Средства контроля и досмотра в деятельности правоохранительных органов

В процессе расследования, при осмотре мест происшествий, производственных помещений, транспорта может возникнуть необходимость в контроле радиационной обстановки, выявлении локальных зон загрязненности радионуклидами, в проверке на загрязненность отдельных предметов. Простейшими приборами, позволяющими оценивать параметры ионизирующего излучения (дозы) являются портативные (карманные) дозиметры, которые должны включаться в оснащение следователя и специалиста.

Более совершенными приборами, отвечающими различным потребностям следственной практики, являются *дозиметры-радиометры,* в частности, приборы типа *«ЭКО» («ЭКО-1», «ЭКО-7).*

Дозиметры-радиометры «ЭКО» имеют три режима работы. Режим F —обнаружение радиации и оценка уровня радиационной безопасности по мощности эквивалентной дозы Y-излучения. В данном режиме возможно циклическое измерение через каждые 20 сек, с подачей звукового сигнала при превышении мощности дозы, равной 60 мкР/ч. Предусмотрено также однократное измерение со звуковой сигнализацией через 20 сек.; этот вариант рекомендуется использовать для поисковых измерений в целях получения информации о наличии источника излучения, резком повышении уровня фона излучения, направлении излучения, а также для выполнения измерений в труднодоступных местах, где затруднено непосредственное визуальное наблюдение по табло прибора (например, в ямах, подвалах и т. п.).

Режим А — определение загрязненности (удельной радиоактивности) почвы, воды, строительных материалов, грузов, почтовых отправлений, продуктов питания, продуктов растениеводства, животноводства, рыболовства и других объектов (проб) излучающими радионуклидами.

Режим В — оценка уровня загрязненности радионуклидами поверхности различных предметов, одежды, тела и других объектов (проб) по плотности потока Р-частиц.

Поскольку показания дозиметров-радиометров фиксируются в протоколе следственного действия и могут иметь доказательственное значение (например, при расследовании экологических преступлений), эти приборы должны ежегодно проходить государственную поверку.

В следственной и оперативно-розыскной работе иногда возникают ситуации, когда приходится проводить поиск людей, укрывающихся в грузах (контейнерах, ящиках, тюках), перевозимых на транспортных средствах. Для решения таких задач предназначены приборы обнаружения «*Лаванда-М*» и «*Гиацинт*». Приборы воспроизводят звуковые колебания, восприятие которых позволяет судить о наличии или отсутствии в осматриваемом транспортном средстве человека.

В современных условиях в деятельности правоохранительных органов в ряде случаев приходится принимать меры по выявлению каналов и средств неправомерного завладения секретной, конфиденциальной информацией, сведениями ограниченного доступа. Проверка различных помещений и территорий на обнаружение признаков утечки информации (наличие скрытых радиопередающих и регистрирующих устройств, подключений для криминального использования телефонной и электрической сети и т. д.) осуществляется с применением поисковой аппаратуры, которой располагают специалисты. Некоторые поисковые средства такого назначения иногда включают в передвижные криминалистические лаборатории, их используют для профилактического контроля в помещении правоохранительного органа.

Достаточно совершенным прибором в этой группе является многофункциональный прибор *СРМ-700,* который предназначен для обнаружения каналов утечки информации в широком диапазоне частот. При помощи выносной высокочастотной антенны можно выявить передатчики, установленные в телефонном аппарате, предметах интерьера, технических средствах обработки и передачи данных; определить факт негласного заноса передающего устройства в помещение. Низкочастотной антенной можно обследовать электро- и телефонные линии, а также провода и кабели, которые используются как каналы передачи информации, — таким путем выявляются подключенные к линиям микрофоны. В приборе имеется возможность применения звукозаписи для фиксации выявленных сигналов.

К многофункциональным поисковым средствам указанного назначения относятся также приборы *OSC-5000, VL-5000P.*

Для обнаружения и слухового контроля сигналов от различных передающих устройств используются сканирующие приемники с ручным и автоматизированными режимами работы (например, типа *AR-lSOO, AR-3000A*). Локализация источников радиоизлучений проводится малогабаритными детекторами (индикаторами) радиоизлучений — антенну прибора приближают к месту предполагаемого нахождения передатчика (телефонный аппарат, штепсельная розетка, настольная лампа, ящик стола, декоративный предмет и т. п.), появление звукового и светового сигналов детектора свидетельствует об обнаружении источника излучения. Обследованию подлежат не только внутренние помещения, но и стены, стекла окон снаружи, так как на них могут быть установлены радиостетоскопы.

Факт обнаружения в ходе следственного осмотра или обыска устройств для неправомерного завладения информацией отражается в протоколе этих действий; сами устройства описываются, фотографируются, фиксируются видеосъемкой и изымаются для последующих экспертных исследований.

Рассмотренные научно-технические средства (НТС) не исчерпывают всего многообразия поисковой техники. Постоянно разрабатываются новые приборы, приспособления, химические составы, которые после прохождения экспериментальной проверки внедряются в практическую деятельность правоохранительных органов. Применение НТС в деятельности правоохранительных органов направлено на повышение эффективности борьбы с преступностью. Конкретизация этой общей направленности позволяет выделить более узкие цели использования техники — применение НТС в процессе доказывания, выполнения ОРМ, проведения профилактической работы, научной организации и интенсификации труда в правоохранительных органах, повышения уровня подготовки кадров.

С помощью современных технических средств установленные фактические данные надежно защищаются от необоснованного дезавуирования, фальсификации, искажения, подмены, уничтожения, неправомерного использования. При производстве следственных действий технические средства применяются для решения задач обнаружения следов и предметов, их осмотра, фиксации, изъятия, упаковки, удостоверения. Результаты применения НТС в процессуальной форме, зафиксированные в установленном законом порядке, могут иметь судебно-доказательственное значение по уголовному делу.

В процессе доказывания по уголовным делам могут найти применение технические средства и методы, которые основаны на подлинно научных достижениях, прошли экспериментальную проверку и признаны судебно-следственной практикой. Традиционный собирательный термин «научно-технические средства» означает, что средства и методы их криминалистического применения должны иметь научную основу, базироваться на изученных объективных закономерностях. Не могут использоваться в доказывании устройства, основанные на неустановленных наукой явлениях, результаты применения которых неоднозначны и зависят от субъективного толкования лицами с действительными или мнимыми экстраординарными способностями (например, индикаторы, применяемые экстрасенсами, телепатами и т. п.).

Тема 2. СОВРЕМЕННЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА НАБЛЮДЕНИЯ

Технические средства наблюдения (ТСН) предназначены для обеспечения контроля и безопасности в зданиях, помещениях, на охраняемых территориях и в других местах. Они позволяют одному или нескольким наблюдателям одновременно следить за одним или многими объектами, находящимися порой на значительном расстоянии как друг от друга, так и от места наблюдения.

В настоящее время ТСН не являются экзотикой. Стоимость наиболее простых систем позволяет их использовать в качестве, например, дверного глазка.

Существует целый ряд применений ТСН в научных исследованиях и в промышленности, например, для контроля за технологическими процессами и управления ими. При этом наблюдения могут производиться в условиях очень низкой освещенности и любой не приемлемой для нахождения людей среды.

ТСН подразделяются на две основные категории:

- средства дистанционного наблюдения (телевизионные системы наблюдения);
- средства непосредственного наблюдения.

§ 1. Системы телевизионного наблюдения

Любое средство охранной сигнализации в ответ на внешнее воздействие, характерное для нарушителя, находящегося в охраняемой зоне, вырабатывает сигнал тревоги с определенной вероятностью. Существует и возможность ложной подачи тревоги — Р ложной тревоги. Это вызывает необходимость наличия средства идентификации оператором процессов, происходящих в охраняемых зонах и на подступах к ним. В качестве таких средств наиболее оптимально с позиций восприятия человеком-оператором применение *телевизионной аппаратуры замкнутых видеосистем.*

Такие системы, включающие аппаратуру видеонаблюдения и средства охранной сигнализации, относятся уже к интегрированным системам охраны (ИСО). В наиболее полном варианте ИСО включают в себя пожарную сигнализацию, аппаратуру контроля доступа, инженерные средства защиты и т. д.

Телевизионные системы видеоконтроля играют наиболее существенную роль в структуре ИСО, так как выводят систему охраны объекта на качественно более высокий уровень. Ценность телевизионных систем видеоконтроля состоит в том, что они позволяют получить визуальную картину состояния охраняемого объекта, обладающую такой высокой информативностью, какую не могут дать никакие другие технические средства охраны. При этом сотрудник службы безопасности находится вдали от зоны наблюдения. Это создает ему условия для достаточно спокойного анализа получаемой информации и принятия обдуманного решения.

Наиболее простая система телевизионного наблюдения включает телевизионную камеру и монитор. Камера может быть подключена непосредственно к телевизору или монитору.

Для небольшого объекта охраны достаточно не более четырех-пяти камер. Используя монитор с встроенным коммутатором и удачно расположив камеры, обеспечивается круглосуточное наблюдение за охраняемой территорией.

Количество одновременно отображаемых камер должно быть ограничено. При увеличении количества мониторов оператору трудно следить за всеми изменениями. В многокамерных системах используются дополнительные устройства.

К дополнительным устройствам относятся детекторы движения, которые анализируют изменения изображения, например, перемещения любого предмета в поле зрения камеры, и сигнализируют оператору об этом.

Для дистанционного управления камерами используются поворотные устройства. Они позволяют увеличить обзор камеры посредством ее поворота в двух плоскостях. Управление поворотными устройствами может осуществляться джойстиком.

Для одновременного получения нескольких изображений (до 16) на экране одного монитора используются *квадраторы* («делители экрана»). Квадраторы преобразуют сигналы от нескольких видеокамер в изображение, которое отображается на одном мониторе. При этом изображение от любой камеры можно оперативно развернуть на весь экран. Квадраторы получили свое название из-за того, что первые модели делили экран на 4 окна и в каждом отображалась одна из камер. Для последовательного вывода на экран изображения от нескольких камер в системах телевизионного наблюдения используются мультиплексоры (коммутаторы). В режиме просмотра они последовательно подключают камеры к монитору. Для оперативной работы оператор имеет возможность вывести на экран любое изображение или исключить любую камеру. Периодичность переключения и время наблюдения изображения задается для всех камер одновременно. На крупных объектах число камер может составлять несколько десятков. Для повышения эффективности работы оператора используют матричные коммутаторы. Они позволяют создать гибкую и наращиваемую систему безопасности, в которую могут входить не только компоненты телевизионных систем, но и системы сигнализации и контроля доступа. Запись видеоизображения может осуществляться на специализированные видеомагнитофоны в традиционных системах или в цифровой форме при помощи компьютера. Специализированные видеомагнитофоны позволяют записывать изображение через несколько кадров (старт-стопный режим). В результате время записи увеличивается. На обычной кассете VHS (180 минут) продолжительность записи может составлять до 960 часов. Все устройства объединяются в систему, которая обеспечивает возможность оперативного наблюдения. Управление системами телевизионного наблюдения в зависимости от их сложности и обстановки на объекте может быть автоматическим или ручным. Компьютерные системы телевизионного наблюдения обладают рядом особенностей, которые в различных ситуациях могут играть как положительную, так и отрицательную роль. Перераспределение функций между программными и аппаратными средствами приводит к тому, что компьютерные системы не всегда могут обеспечить быстрое переключение режимов. Кроме того, повышаются требования к оператору — умение работать с компьютером и графическим интерфейсом.

Любая система телевизионного наблюдения включает три функциональные части:

- телевизионные камеры;
- аппаратуру обработки видеоинформации;
- мониторы.

По способу приема и обработки видеоинформации различают:

- традиционные системы телевизионного наблюдения на базе специализированной аппаратуры;
- компьютерные системы телевизионного наблюдения.

Задача системы телевизионного наблюдения — наглядно представить видеоинформацию об оперативной обстановке контролируемого объекта. Для решения этой задачи, в соответствии с характеристиками контролируемых объектов, выбираются параметры системы.

К основным факторам, определяющим выбор состава системы телевизионного наблюдения, относятся:

- количество контролируемых объектов;
- скорость реакции системы;
- стоимость;
- простота управления и возможность работы в ведомом режиме;
- надежность;
- гибкость.

Параметры элементов системы телевизионного наблюдения выбираются в соответствии с характеристиками объектов:

- размеры объектов;
- среднее расстояние до объектов;
- скорость перемещения объектов;
- условия освещения объектов.

В системах телевизионного наблюдения максимальное количество одновременно отображаемых камер ничем не ограничивается и определяется в каждом случае соотношением количества мониторов и возможностями устройств обработки видеоинформации.

Обычно более половины камер отображаются одновременно, а остальные — просматриваются в режиме пролистывания.

Сложные системы телевизионного наблюдения позволяют получить на телевизионных или компьютерных мониторах видеоизображение от большого числа точек охраняемого объекта. Мониторы и оборудование обработки видеосигналов устанавливаются в дежурных помещениях или у сотрудников фирмы, курирующих службу безопасности.

В компьютерных системах на одном мониторе отображается не более 16 камер. При бóльшем числе камер размеры отдельных изображений сильно уменьшаются, а видеоканалы переключаются в режиме пролистывания блоками до 16 камер одновременно.

Наглядность представления оперативной обстановки выше в системах с большим количеством мониторов, так как при этом возможно отображение всех камер одновременно с изображением нужного размера.

Скорость обработки видеоинформации близка к обработке в масштабе реального времени и при оптимальном составе средств обработки видеоинформации не зависит от количества камер.

В компьютерных системах скорость обработки видеоинформации уменьшается по мере роста количества камер. Скорость реакции аппаратуры на действия оператора выше в традиционных системах.

Методы цифровой обработки позволяют улучшать видеоизображение, фильтровать шумы, выделять и исследовать отдельные детали.

Состав системы выбирается исходя из количества объектов наблюдения, стоимости, требований к простоте управления и скорости реакции системы.

Одну и ту же задачу можно решить, используя разные конфигурации систем. Средняя стоимость черно-белой камеры, в среднем, такая же, как и поворотного устройства. Следовательно, экономически целесообразно использовать камеру

с поворотным устройством в случае, если необходим угол обзора более 180° (угол обзора 180° можно обеспечить двумя камерами).

Скорость перемещения поворотного устройства находится в пределах 0...12° в секунду. При выбранном среднем расстоянии до объекта, например, 10 м, можно отслеживать перемещения предметов, движущихся со скоростью не более 2 м/с.

В зависимости от количества объектов, предполагаемой наибольшей скорости их перемещения (человек — 10 м/с, машина — 30 м/с) — выбирается необходимая скорость реакции системы. При этом так же следует учесть скорость реакции оператора.

Дополнительные устройства систем телевизионного наблюдения позволяют дублировать некоторые функции оператора, увеличивая надежность, и увеличить скорость реакции системы, привлекая внимание оператора и включая исполнительные устройства.

Для увеличения скорости реакции дополнительные устройства имеют «тревожные» входы и выходы. «Тревожные» входы предназначены для включения дополнительного устройства, например, мультиплексора.

Мультиплексор переключается в такое состояние, чтобы на мониторе отображалось видеоизображение «тревожной зоны».

«Тревожные» выходы предназначены для включения исполняющих устройств. Это может быть освещение, сирена и пр.

Возможность работы системы в ведомом режиме обусловлена необходимостью дублирования некоторых функций оператора. Использование, например, датчиков движения позволяет автоматически непрерывно контролировать любое количество видеоизображений. Независимо от действий оператора система может включать видеомагнитофон, освещение и другие устройства.

§ 2. Элементы систем телевизионного наблюдения

Качество изображения определяется, прежде всего, телевизионной камерой. Она представляет собой законченное устройство, которое, будучи подключенным к видеовходу монитора или телевизора, позволяет наблюдать изображение на экране на значительном расстоянии от объекта съемки. В настоящее время выпускаются видеокамеры для систем телевизионного наблюдения (включая модификации), отличающиеся: характером изображения (черно-белое или цветное); четкостью изображения; светочувствительностью (минимальной рабочей освещенностью объекта съемки); возможностью цифровой обработки видеосигнала; допустимыми климатическими условиями работы; напряжением питания. С целью обеспечения качественной работы в условиях переменной яркости изображения и различных уровней фоновых засветок современные телекамеры, для систем телевизионного наблюдения, оснащаются подсистемами компенсации этих воздействий. Камеры с ручной регулировкой или вообще без соответствующей подсистемы выпускаются в основном для научных приложений. В целях увеличения сектора обзора, телевизионные камеры устанавливают на поворотные устройства с горизонтальным или с горизонтальным и вертикальным сканированием. При повороте камеры следует учитывать возможные реакции систем компенсации внешних воздействий (засветка, воздействие импульсных источников искусственного освещения и т. д.). При установке на улице телекамеры помещаются в специальные защитные корпуса. Вторым важным элементом систем видеонаблюдения является видеомонитор. Он

должен обеспечивать высокую долговременную стабильность и не требовать регулярной калибровки. Надежность также зависит от того, насколько оптимальны схемные решения, прочна и удобна механическая конструкция.

В дополнение к основным устройствам обработки широко применяются различные вспомогательные устройства: кабельные усилители — для компенсации потерь в кабеле при передаче видеосигнала на расстояние до 2 км; разветвители, позволяющие к одной телекамере подключать несколько мониторов, видеомагнитофонов и т. п.; генераторы вспомогательной текстовой информации (даты, времени, номера или идентификатора камеры и т. п.).

Телевизионные камеры. Телевизионная камера — это устройство, которое преобразует оптическое изображение наблюдаемого объекта в электрический видеосигнал определенного стандарта. Телекамера является важнейшим элементом системы, так как именно с нее в систему поступает первичная информация об объекте и именно ее характеристиками определяется качество изображения в целом. Камера представляет собой электронную плату, на которой размещены чувствительный элемент — матрица, выполненная на приборах с зарядовой связью, и объектив. Более простые камеры оснащаются, как правило, простейшими встроенными объективами, более дорогие — сменными объективами с улучшенными характеристиками и широкими функциональными возможностями.

Камеры различают:

- корпусные и бескорпусные;
- черно-белого и цветного изображения;
- обычной и повышенной чувствительности;
- обычного и высокого разрешения;
- для внутреннего и наружного наблюдения;
- для скрытого наблюдения.

Качество телекамеры определяется целым рядом показателей, однако в большинстве случаев при выборе камеры для конкретной системы достаточно ориентироваться на следующие ее характеристики.

Преобразователи свет-сигнал представляют собой либо передающие электронно-лучевые ТВ трубки (ЭЛТ), либо твердотельные матрицы — так называемые «приборы с зарядовой связью» (ПЗС).

Оптический формат — размер фоточувствительной области ПЗС-матрицы в дюймах. Основные форматы: 1/3", 1/2", 2/3" и 1". Чем больше оптический формат, тем меньше геометрическое искажение изображения. В особенности это сказывается при больших углах зрения. В ТСВ среднего и высокого классов обычно используются ПЗС-матрицы формата 1/2", 2/3" и 1". Камеры с оптическим форматом 1/3" имеют небольшие габариты и стоимость и используются, в основном, для скрытого наблюдения, а также в системах с невысокими требованиями к качеству изображения. В последнее время на рынке появились миниатюрные камеры с ПЗС-матрицей формата 1/4".

Разрешающая способность — максимальное количество телевизионных линий, различаемых визуально в выходном сигнале камеры при минимально допустимой глубине модуляции 10 %. Разрешение по горизонтали определяет максимальное количество градаций от черного к белому или обратно, которые могут быть получены от камеры в центральной части экрана. На краях экрана допускается некоторое ухудшение качества изображения. Чем выше разрешение камеры, тем более мелкие детали можно различить на изображении. Обычным разрешением считается 380...420 ТВЛ для черно-белых и 300...320 ТВЛ для цветных камер.

В системах высокого класса используются, как правило, камеры с повышенным разрешением.

Пороговая чувствительность — минимальная освещенность на ПЗС-матрице, при которой камера сохраняет работоспособность. Обычной чувствительностью считается 0,1...0,5 лк для черно-белых и 1...3 лк для цветных камер.

В системах, предназначенных для наблюдения слабо освещенных объектов, имеющих малую отражающую способность, используются камеры высокой чувствительности.

ПЗС-матрицы обладают очень важным свойством — они позволяют получать четкое изображение в условиях полной темноты при подсветке инфракрасными лучами. С этой целью некоторые камеры оснащаются встроенной ИК-подсветкой.

Синхронизация — привязка видеосигнала к фазе сетевого напряжения или внешнего источника синхроимпульсов или другого видеосигнала. Как правило, в реальных ТСВ видеосигналы нескольких камер с помощью специальных устройств по заданной программе коммутируются на один монитор, поэтому необходимо, чтобы переключение камер происходило в начале кадра. Камеры, питающиеся от сети переменного тока, синхронизируются от питающей сети. Камеры, питающиеся от источника постоянного тока, должны иметь вход внешней синхронизации, сигнал на который подается от специального устройства — синхронизатора. Отсутствие внешней синхронизации телекамер от единого источника синхронизации в значительной степени повышает утомляемость оператора ТСВ, а при использовании в системе более 8 камер приводит к постоянным срывам изображения, потерям кадров, что делает наблюдение и видеозапись практически невозможными.

Электронный «затвор» — элемент электронной части ПЗС-матрицы, обеспечивающий возможность изменения времени накопления электрического заряда. Электронный «затвор» позволяет получить приемлемое качество изображения быстродвижущихся объектов и обеспечивает работоспособность камеры в условиях высокой освещенности. Обычные электронные «затворы» обеспечивают регулировку выдержки в диапазоне от 1/50 до 1/10 000 ... 1/15 000 с. «Суперзатворы» позволяют получать выдержки порядка 1/100 000 с.

Электронная диафрагма — элемент электронной части ПЗС-матрицы, обеспечивающий автоматическую регулировку выдержки в зависимости от уровня освещенности. Принцип действия электронной диафрагмы аналогичен принципу действия электронного «затвора». Как правило, в камерах с электронной диафрагмой имеется возможность ее отключения.

Автоирис — способность камеры управлять объективами с электромеханически регулируемой диафрагмой и встроенным усилителем. Наличие автоириса — существенное достоинство камеры, так как регулировка глубины резкости без изменения диафрагмы принципиально невозможна. Это означает, что при электронном управлении «затвором» в ПЗС-матрице изображение объекта, находящегося на расстоянии, отличном от фокусного, будет недостаточно резким. Кроме этого, отсутствие регулировки диафрагмы приводит к резкому уменьшению диапазона управления световым потоком.

Автоматическая регулировка усиления — свойство электронной части камеры изменять коэффициент усиления в видеотракте в зависимости от уровня видеосигнала. АРУ сглаживает изменения уровня сигнала и позволяет получить приемлемую «картинку» на мониторе при недостаточной освещенности объекта. Обычно диапазон регулировки ограничивается 12...20 дБ, так как большее увеличение уси-

ления приводит к значительному зашумлению видеосигнала и, как следствие, ухудшению изображения.

Отношение сигнал/шум. Позволяет учитывать, когда требуется высокое качество телевизионного сигнала — чем оно выше, тем выше качество изображения. Обычным является отношение сигнал/шум 40 дБ. У камер высокого класса это отношение достигает 58 дБ, что позволяет доводить АРУ до 45 дБ и выше.

Гамма-коррекция видеосигнала — внесение нелинейных искажений в видеосигнал для лучшего воспроизведения. Гамма-коррекция заключается в предыскажении видеосигнала с целью увеличения контрастности изображения на мониторе. Камеры с γ-коррекцией сигнала имеют либо постоянный коэффициент γ = 0,45, либо изменяемый вручную.

Компенсация «света сзади» — способность камеры автоматически устанавливать выдержку и параметры усиления по выбранному фрагменту изображения. В достаточно дорогих камерах применяется система Back Light Compensation, обеспечивающая автоматическое управление диафрагмой, выдержкой, усилением и т. д. и ориентирующаяся на оптимальное качество передачи центральной части кадра.

Канал звука — обеспечивает акустический контроль контролируемого помещения с помощью встроенного в камеру монофонического микрофона. Для организации двунаправленного аудиоканала в камеру кроме микрофона встраивается динамическая головка.

Конструкция узла присоединения объектива. Если камера не имеет встроенного объектива, то в ее конструкции предусмотрен узел присоединения для установки сменных объективов. При выборе объектива для камеры следует учитывать, что применяются два типа стандартных конструкций узлов присоединения:

– тип С — резьба 2,54 × 0,8 мм и расстояние от задней плоскости объектива до опорной плоскости ПЗС-матрицы 17,5 мм;

– тип CS — резьба 2,54 × 0,8 мм и расстояние до опорной плоскости матрицы 12,5 мм. Этот тип крепления находит большее распространение в связи с тенденцией камер к миниатюризации. Миниатюрные камеры для скрытого наблюдения имеют специальную насадку с оптоволоконным кабелем, на конце которого крепится объектив с диаметром светового зрачка от 0,9 до 2,0 мм.

Напряжение питания. Большинство телекамер питаются либо от сети переменного тока 220 В / 50 Гц, либо от источников постоянного тока напряжением 12 В. Реже используется переменное напряжение 24 В и постоянное напряжение 9 В. Для питания нескольких камер в системе могут использоваться индивидуальные для каждой камеры источники, либо общий источник. Необходимо иметь в виду, что цветные камеры очень чувствительны к перепадам напряжения в питающей сети, поэтому следует применять специальные стабилизированные источники.

Узел крепления телекамеры к несущим деталям — предназначен для фиксации конструкции телекамеры в кожухе, на кронштейне, поворотном устройстве и т. п.

Для камер цветного изображения важны такие характеристики как автоматический баланс белого и стандарт кодирования светового сигнала.

В ТСВ в основном применяются камеры черно-белого изображения. Это объясняется тем, что они значительно дешевле цветных и работают с более дешевым оборудованием, имеют более высокое разрешение и чувствительность, не предъявляют жестких требований к источнику питания. Цветные камеры устанавливаются главным образом там, где требуется знать цвет объекта.

Камера Panasonic WV-CP220/222/224

- WV-CP220 (питание от сети).
- WV-CP222 (12 В постоянного тока).
- WV-CP224 (24 В переменного тока).
- 1/3-дюймовая ПЗС-матрица (512H × 582V) с горизонтальной четкостью 330 твл с микролинзами на каждом пикселе.
- Чувствительность 1,1 лк (F1,2), 0,4 лк (F0,75).
- Переключение четкости изображения: четко/мягко.
- Синхронизация: Gen Lock (внешн.), VD2, INT (внутрен.), LL.
- Крепление типа CS, используются видеообъективы/системы привода постоянного тока.
- Автоматические функции ALC/ELC.

Объективы. Объектив — это устройство, формирующее изображение объекта в плоскости ПЗС-матрицы. Он может быть встроенным или сменным. Для камер с присоединительным узлом C подходят только объективы типа C. Если камера имеет узел CS, то к ней подходят не только объективы CS, но и C со специальным переходным кольцом. Подбирая объективы к камере, надо иметь в виду, что обычно они рассчитываются на ПЗС-матрицу определенного формата.

Фокусное расстояние f — характеризует величину угла зрения при определенном оптическом формате камеры. Чем меньше фокусное расстояние, тем больший угол зрения наблюдаемого пространства можно получить и наоборот. Однако при очень больших углах зрения довольно сложно, а порой и невозможно, рассмотреть детали картины. Наиболее приемлемым для оператора является угол зрения 60...70°, так как получаемое при этом изображение хорошо согласуется с характеристиками человеческого зрения. Объективы с большим фокусным расстоянием используются, когда требуется получить четкое изображение мелких деталей.

Трансфокатор — устройство, позволяющее изменять фокусное расстояние в широких пределах. Объективы, снабженные трансфокаторами, называются вариообъективами. Фокусное расстояние может изменяться вручную либо путем сервоуправления. Вариообъективы ввиду их большой стоимости применяются только в тех случаях, когда необходимо быстро увеличить изображение мелкой детали.

Относительное отверстие F определяет освещенность на ПЗС-матрице. В технической документации на телекамеру иногда указывается ее чувствительность при относительном отверстии объектива, с которым она используется.

Возможность регулирования диафрагмы. Различают объективы с ручным управлением диафрагмой и с автодиафрагмой. Объективы с автодиафрагмой позволяют получать качественное изображение как при ярком солнце, так и при низкой освещенности и применяются в тех случаях, когда освещенность объекта в течение периода наблюдения может меняться в широких пределах либо не исключены полностью прямые засветки камеры. В системах обычного класса удовлетворительный результат можно получить, применяя объективы с постоянной диафрагмой и камеры с электронным затвором, что значительно дешевле.

Кожухи для внутренних и внешних применений. По конструктивному признаку телевизионные камеры можно подразделить на корпусные и бескорпусные. Бескорпусные камеры имеют значительно меньшие габариты и стоимость по сравнению с камерами в корпусе и предназначены для систем скрытого наблюдения. Камеры для открытого внутреннего наблюдения размещаются в защитных корпусах, которые имеют разную форму, габариты, конструкцию крепления и по-

зволяют выбрать оформление, наиболее подходящее к конкретному интерьеру. Камеры для использования на открытом воздухе помещаются в защитные кожухи, оборудованные подогревом — гермокожухи. Гермокожухи предназначены для работы в широком диапазоне климатических условий и позволяют использовать различные комбинации телекамер и объективов. Кожух снабжен солнцезащитным козырьком, платой для установки камеры, термостатом и коммутационной панелью. Некоторые гермокожухи имеют дополнительное оборудование — вентиляторы, дворники, омыватели стекла. Следует отметить, что импортные нагреватели не всегда отвечают российским климатическим условиям и не рассчитаны на сильные морозы.

Поворотные устройства, устройства инфракрасной подсветки, кронштейны. Поворотные устройства предназначены для телекамер с дистанционным управлением. Они обеспечивают поворот в горизонтальной и вертикальной плоскостях либо только в горизонтальной. Различают поворотные устройства с постоянной и с регулируемой угловой скоростью перемещения. Сигналы управления камерами преобразуются в заданные механические перемещения с помощью приемников телеметрических сигналов управления.

Как правило, вместе с поворотными устройствами поставляются пульты управления, с помощью которых можно манипулировать также трансфокаторами объективов, если требуется получить укрупненное изображение.

Устройства инфракрасной подсветки. Для обеспечения работоспособности камеры в полной темноте используются устройства местной ИК-подсветки и ИК-прожекторы, осуществляющие облучение наблюдаемого объекта инфракрасными лучами. Однако эти устройства дают небольшой угол подсветки, что не позволяет качественно контролировать всю зону. Кроме этого, ИК-прожекторы достаточно дороги.

Кронштейны служат для крепления камер к стенам, панелям и другим несущим конструкциям и позволяют точно ориентировать поле зрения камеры в нужном направлении. Различают кронштейны для горизонтальной поверхности, для вертикальной поверхности, телескопические и т. п. Исполнение кронштейнов определяется, главным образом, эстетическими требованиями и нагрузкой: на кронштейнах для внутреннего применения крепятся камеры в несколько сотен граммов, на кронштейнах для уличного применения — массой несколько килограммов.

Устройства обработки и коммутации видеосигналов, видеомониторы — это устройства, преобразующие видеосигналы в двухмерное изображение. Видеомониторы являются изделиями, специально предназначенными для использования в ТСВ, поэтому замена их обычными приемниками телевизионного изображения недопустима. Кроме того, многие видеомониторы снабжены встроенными устройствами для приема сигналов от нескольких камер — видеокоммутаторами. Мониторы делятся на два класса — мониторы черно-белого и цветного изображения. Основные характеристики мониторов — размер экрана по диагонали и разрешающая способность по горизонтали. В ТСВ наиболее часто применяются мониторы с размером экрана 9" и 12". При использовании устройств совмещения изображения применяются, как правило, мониторы с большим размером экрана: 15", 17" или 20". Выбирать монитор по разрешающей способности следует таким образом, чтобы она была выше, чем у применяемых телекамер, монитор не должен ухудшать общее разрешение системы. При использовании в системе камер с обычным разрешением целесообразно выбрать монитор с обычным разрешением. В системах высокого класса, как правило, используются мониторы с разрешением 900...1000 ТВ-линий

и 450...500 ТВ-линий. При наличии в системе нескольких мониторов они, как правило, размещаются в специальных стойках.

Видеокоммутаторы последовательного действия. Видеокоммутаторы — это устройства, обеспечивающие последовательное переключение видеосигналов от нескольких телекамер на один или несколько выходов. Видеокоммутаторы последовательного действия имеют автоматический и ручной режимы переключения камер, позволяющие просматривать сигналы от всех камер либо выборочно от некоторых из них. Число входных видеосигналов может быть от 4 до 16, а при использовании нескольких блоков коммутации — до 64. Однако на практике обычно используются коммутаторы на 4 или 8 входов, так как в системах с большим числом камер целесообразно использовать более сложную аппаратуру, имеющую расширенные функции, возможность программирования и т. п. При выборе коммутатора следует обратить внимание на то, чтобы он имел регулировку времени просмотра видеокадров от камер. Желательно наличие входов для подключения средств охранной сигнализации и один или несколько контактных выходов «Тревога». При срабатывании охранной сигнализации система из режима «листания» переходит в режим просмотра той камеры, в поле зрения которой произошло нарушение, что позволяет оператору получить исчерпывающую информацию о нарушении и принять соответствующие меры. Некоторые видеокоммутаторы имеют так называемый «залповый» режим работы, в котором изображения на мониторах формируются как связанные, синхронно переключающиеся между собой группы. Эта функция позволяет оператору увидеть охраняемый участок целиком перед тем, как перейти к следующему. Видеокоммутаторы последовательного действия являются сравнительно простыми устройствами и применяются, как правило, в небольших и недорогих системах.

Видеоквадраторы — это цифровые устройства, обеспечивающие размещение изображений от 4 видеоисточников на одном экране, который в этом случае делится на 4 части, и позволяющие уменьшить количество мониторов в системе. Квадраторы высокого разрешения позволяют работать на одном мониторе с 8 камерами: они формируют две группы по 4 камеры и дают возможность по очереди выводить их на экран. Различают видеоквадраторы «реального времени», обеспечивающие одновременную смену изображений во всех 4 квадрантах, и видеоквадраторы последовательного типа, обеспечивающие скорость смены изображений в каждом квадранте в 4 раза ниже номинальной частоты полей. Большинство квадраторов могут работать как коммутатор последовательного действия, т. е. подключать любую из работающих камер к монитору. Квадраторы для ТСВ должны иметь дополнительные «тревожные» входы для подключения средств сигнализации и обеспечивать вывод камеры на полный экран при срабатывании в ее зоне наблюдения средств сигнализации, режим «заморозки» кадра, т. е. возможность зафиксировать изображение в одном из сегментов, передачу сигнала тревоги прочим потребителям и, при необходимости, запись на видеомагнитофон. Видеоквадраторы, как и видеокоммутаторы последовательного действия, — сравнительно простые устройства и применяются, как правило, в небольших и недорогих системах.

Видеодетектор движения — представляет собой электронный блок, который хранит в памяти текущее изображение с телекамеры и подает сигнал тревоги при возникновении изменений в охраняемой зоне. Видеодетекторы применяются, главным образом, в системах охраны крупных объектов, где оператору приходится контролировать большое количество камер. Различают аналоговые и цифровые детек-

торы движения. Наиболее простыми и дешевыми являются аналоговые детекторы, действие которых можно, при некоторых допущениях, сравнить с действием охранных извещателей, подключаемых к тревожным входам коммутаторов, квадраторов и т. п. Цифровые видеодетекторы движения — это многоканальные устройства, которые позволяют разбивать каждую охраняемую зону на отдельные блоки, для каждого из которых устанавливается свой порог срабатывания — чем выше этот порог, тем бóльшие изменения должны произойти на «картинке». Кроме этого, характеристики движения можно задавать программным путем. Это позволяет, например, не воспринимать человека, движущегося в направлении от охраняемого объекта либо параллельно ему на некотором безопасном расстоянии, как нарушителя. Настройка системы с цифровыми детекторами на оптимальный режим должна производиться с учетом особенностей места установки телекамеры и характеристик охраняемого объекта, иначе трудно избежать большого количества ложных срабатываний или, наоборот, пропуска нарушителя. Цифровые видеодетекторы движения применяются в сложных ТСВ высокого класса.

Видеомультиплексоры — представляют собой высокотехнологические системы видеозаписи и управления, обладающие широкими функциональными возможностями. Они предназначены для записи видеосигналов от нескольких камер на одну видеокассету, воспроизведения кодированных кассет и обработки сигналов тревоги. Мультиплексоры позволяют осуществлять переключение между различными методами записи, что дает возможность либо записывать то, что появляется на экране, либо просматривать на экране изображения от одних камер, записывая в это же время изображения от других камер. Благодаря наличию нескольких режимов вывода изображений на экран записанные изображения могут просматриваться на одном мониторе в полноэкранном режиме, режимах квадрированного экрана и «картинка в картинке» либо в мультиэкранном режиме. Для более подробного анализа полноэкранных изображений многие мультиплексоры имеют функцию двукратного цифрового увеличения изображения. Некоторые мультиплексоры имеют встроенные видеодетекторы движения, генераторы титров, даты и времени, а также могут работать в дуплексном режиме, т. е. позволяют просматривать ранее сделанные записи одновременно с текущей записью изображений с работающих телекамер. Широкий набор встроенных функций, развитая логика обработки сигналов тревоги, а также возможность программирования видеомультиплексоров с помощью функциональных клавиш или с персонального компьютера позволяют создавать на их базе средние и большие телевизионные системы видеоконтроля, для чего ведущими фирмами разработан целый спектр дополнительной аппаратуры: адаптеры удаленной клавиатуры, многопортовые контроллеры, системы телеметрического управления камерами и т. п.

Матричные видеокоммутаторы имеют встроенный процессор и обеспечивают независимую коммутацию видеосигналов с большого количества входов на любой из мониторов. При наличии детектора движения коммутатор самостоятельно отслеживает ситуацию и в случае тревоги выводит изображение именно того помещения, где сработала сигнализация, а также выдает звуковой сигнал для привлечения внимания оператора. Матричные коммутаторы позволяют формировать несколько последовательностей изображений от камер в любом порядке с управлением их поворотными устройствами и вариообъективами, а также выводить номера камер и названия помещений, в которых они установлены, сообщения о сигналах тревоги, текущее время, дату, инструкции оператору и т. п. Матричные коммутаторы являются основными элементами многих ТСВ, так как позволяют

создавать гибкие и наращиваемые системы безопасности, в которые могут входить не только телевизионные компоненты, но и системы сигнализации и контроля доступа.

Устройства регистрации

Специализированные видеомагнитофоны. Предназначены для регистрации и документирования в течение длительного времени событий, происходящих в охраняемых зонах. Они ведут непрерывную запись в течение 3...960 часов на стандартную видеокассету. Одним из важных параметров видеомагнитофона является его разрешающая способность при записи изображения и надежность его работы.

На передней панели под крышкой находятся органы управления, с помощью которых можно установить различные режимы работы: запись, воспроизведение, обратное воспроизведение, стоп-кадр, быструю перемотку ленты в двух направлениях, размещение информации по времени и дате в любом месте на экране, коррекция показаний времени и даты. Видеомагнитофон запоминает время и дату момента подачи внешних сигналов и позволяет индексировать записи по сигналу тревоги с последующим выборочным воспроизведением по номеру индекса.

Специализированные видеомагнитофоны работают в «старт-стопном» режиме. В зависимости от установленного времени записи на видеопленке фиксируется, например, один из пяти кадров. Таким образом, увеличивается фактическое время записи. Видеомагнитофон включается в общую систему охраны и может программироваться на изменение скорости записи в случае тревоги. Для этого он содержит программируемый таймер. Просмотр записи на мониторе позволяет восстановить события как с целью выявления нарушителя, так и анализа действий охраны в случае тревоги.

Функциональные возможности специализированных видеомагнитофонов: запись и воспроизведение черно-белого или цветного изображения; программирование режимов записи (3 ч, 12 ч, 24 ч, ..., 960 ч); вывод на экран времени и даты; осуществление записи по таймеру или по внешнему сигналу; программирование таймера с установкой ежедневного начала и окончания записи, а также установка режима записи на неделю; специальные режимы воспроизведения (покадровое воспроизведение, пауза, скоростной поиск вперед и назад); стоп-кадр; выдача сигналов синхронизации на внешние устройства; программирование режимов работы при срабатывании сигнализации; регистрация времени аварийного отключения питания; хранение информации в энергонезависимой памяти (табл. 2.2.1). В многокамерных системах видеонаблюдения видеомагнитофоны используются совместно с видеокомпрессорами и мультиплексорами.

Таблица 2.2.1 — Режимы работы видеомагнитофонов

Режим работы	Запись на одну кассету		
	Записываются кадры	Продолжительность записи, ч	Количество кадров за 1 с
Непрерывный	Все	3	25
Прерывистый	Каждый 8-й	24	3
	Каждый 160-й	480	1/7
	Каждый 320-й	960	1/14

При документировании видеозаписи должен использоваться генератор даты-времени, с помощью которого отмечается текущее время суток и дата. Важными характеристиками видеомагнитофона являются его разрешающая способность и надежность. Высокое разрешение позволяет зафиксировать даже мелкие детали, а надежность важна потому, что такие видеомагнитофоны предназначены для непрерывной работы в течение нескольких лет.

Видеопринтеры. Предназначены для оперативной распечатки выбранного кадра от источника видеосигнала. Основными характеристиками видеопринтеров являются разрешающая способность, размер снимка и возможность многокадровой печати.

Устройства передачи телевизионного сигнала. Каналы передачи телевизионного сигнала. Для передачи телевизионного сигнала в ТСВ могут использоваться как проводные каналы связи, так и беспроводные каналы — радиоканал или ИК-канал. Наиболее стабильная и качественная работа системы возможна только при использовании коаксиальных кабелей. Основные характеристики кабеля — волновое сопротивление, диаметр и погонное затухание. Как правило, входные и выходные сопротивления основных компонентов ТСВ имеют значение 75 Ом, т. е. рассчитаны на применение кабелей с волновым сопротивлением 75 Ом, поэтому применять для передачи видеосигнала кабели с волновым сопротивлением 50 Ом не следует. Максимальное расстояние от видеокамеры до приемника видеосигнала зависит от типа используемого кабеля: для РК-75-4 оно не превышает 200 м, для РК-75-7 — 500 м. Выбору коаксиального кабеля для внешнего использования следует уделять особое внимание. Эти кабели должны работать в широком диапазоне температур, быть устойчивыми к воздействиям солнечного света, радиации, агрессивных сред, иметь броневую оплетку для защиты от механических повреждений. Необходимо учесть, что разводка таких кабелей должна производиться в специально выпускаемых для наружного применения кабелепроводах, в которых коаксиальный кабель может быть проложен совместно с проводами питания. При необходимости передачи сигнала на большие расстояния применяются видеоусилители и модемы. При этом видеосигнал с помощью специальной аппаратуры преобразуется, запоминается и передается с использованием модема. Время передачи может составлять от долей секунды до минуты, в зависимости от требований к качеству «картинки». В настоящее время наиболее широко используются три системы передачи изображений по цифровым и обычным телефонным линиям:

– системы с компрессией изображений по принципу «условного» обновления, предназначенные для передачи информации только об изменении изображения от кадра к кадру;

– системы с MPEG-компрессией, в которых используют специальные алгоритмы компрессии изображений движущихся объектов;

– системы с JPEG-компрессией, которые обеспечивают независимое сжатие кадра изображения.

В специальных ТСВ, когда требуется повышенная помехозащищенность информации и высокая разрешающая способность, применяются волоконно-оптические линии связи. Дальность действия таких систем практически не ограничена. Относительная дороговизна их обусловлена тем, что видеокамеры не имеют выхода для подключения оптоволоконного кабеля, поэтому требуется вводить в систему преобразователи электрического сигнала в оптический и обратно. Кроме этого, прокладка, сращивание и подключение достаточно сложны. Однако развитию волоконно-оптических систем в последнее время уделяется повышенное внимание.

При создании мобильных и переносных систем, а также в случаях, если прокладка кабельных линий невозможна или нецелесообразна, используются радио- или инфракрасный каналы связи. Дальность передачи при этом составляет от нескольких сотен метров до нескольких километров. В простейшем случае камера подключается к радиопередатчику дециметрового диапазона, а сигнал принимается на обычный телевизор. Вместе с тем такие системы имеют существенные недостатки, например: могут создавать помехи бытовому телевещанию, сигнал в зоне действия передатчика может принимать преступник. Этих недостатков лишены радиосистемы, работающие в сантиметровом диапазоне, а также работающие в инфракрасном диапазоне. Последние не требуют разрешения на применение системы от Государственного комитета по радиочастотам, однако они работают только в зоне прямой видимости, а их дальность действия в значительной мере зависит от оптической плотности среды.

Видеоусилители и видеораспределители. Видеоусилители применяются для компенсации затухания видеосигнала в линиях при передаче его на большие расстояния. При выборе видеоусилителя необходимо знать его входное и выходное сопротивления, а также коэффициент усиления, так как их значениями определяются тип линии передачи и максимальное расстояние, на которое можно передать видеосигнал. Видеораспределители используются при необходимости трансляции видеосигнала нескольким потребителям. Основные характеристики видеораспределителей — входное и выходное сопротивления, а также количество выходов.

Электропитание телевизионных средств видеоконтроля. Основные напряжения питания компонентов систем телевизионного видеоконтроля — 220 В переменного тока частотой 50 Гц и 12 В постоянного тока. От сети переменного тока напряжением 220 В питаются практически все мониторы, коммутаторы, квадраторы, мультиплексоры, видеомагнитофоны, видеопринтеры, поворотные устройства, гермокожухи, а также некоторые камеры. Напряжением 12 В постоянного тока питаются практически все камеры, а также некоторые устройства обработки видеосигнала и поворотные устройства. В редких случаях питание компонентов ТСВ осуществляется напряжением 24 В постоянного и переменного тока, а также 9 В постоянного тока. Для питания отдельных компонентов ТСВ на рынке телевизионной техники предлагается широкий выбор сетевых адаптеров 220/12 В и 220/9 В. Электропитание всей ТСВ должно быть организовано таким образом, чтобы обеспечивать работоспособность системы в автономном режиме, т. е. при пропадании напряжения сети переменного тока. С этой целью питание компонентов осуществляется от источников бесперебойного питания UPS или специализированные, снабженные аккумуляторами блоки питания. Для питания мониторов, видеомагнитофонов и т. п. также часто используют инверторы — приборы, преобразующие постоянный ток напряжением 12 В в переменный ток напряжением 220 В и частотой 50 Гц. При построении ТСВ ее компоненты следует выбирать таким образом, чтобы номенклатура питающих напряжений и потребляемая мощность были минимальными. Организация питания телекамер является одной из проблем в системах с беспроводными каналами связи. С одной стороны можно подавать питание камер по проводам, но тогда проблема прокладки проводов остается, с другой — можно питать камеры от аккумуляторов, однако из-за большого потребления даже у современных камер приходится часто заменять элементы питания.

Следует обратить внимание на два аспекта электрической безопасности. Первый относится к элементам ТСВ, питаемым от сети 220 В: эти устройства должны быть надежно защищены в соответствии с действующими нормативами от послед-

ствий попадания питающего напряжения на элементы конструкции для исключения поражения током сотрудников и обслуживающего персонала. Это особенно важно для оборудования, эксплуатируемого вне помещений.

Второй аспект также касается этой категории оборудования. Он заключается в надежной защите аппаратуры от попадания грозовых разрядов. Это может не только вывести аппаратуру из строя, но и представлять угрозу жизни операторов центра наблюдения.

Во избежание этого не следует устанавливать телекамеры и иное оборудование выше близрасположенных металлических конструкций. Если же исключить такие варианты невозможно, то необходимо обеспечить надежную молниезащиту, подключаемую типовым способом к надежной системе заземления.

Примеры дополнительных устройств систем телевизионного наблюдения:

Видеомагнитофон HS-7300E

- Производитель: Mitsubishi (Япония).
- Формат: VHS.
- Горизонтальное разрешение: 330 ч/б линий, 240 цв. линий.
- Габариты: 425 × 93 × 315.
- Вес: 4.50 кг.
- Система видеозаписи: 6 головок.
- Время перемотки: около 140 сек (кассета 180 мин).
- Сигнал цветности: Время записи/воспроизведения: 960 часов.
- Яркостной сигнал: Время записи/воспроизведения со звуком: 3, 6, 12, 18, 24 часа.
- Формат видеосигнала: Вход/выход.
- Отношение сигнал/шум: видео: лучше, чем 42 дБ, звук: лучше, чем 43 дБ.
- Энергонезависимая память: последние 31 сутки.
- Температура работы: 5 °C ~ 40 °C.
- Питание: 100–230 V + 10 % переменного тока, 50/60 Гц.

Видеокомпрессор MX-87

- Производитель: Robot (США).
- Цветность: цветной.
- Количество видеовходов (камер): 4.
- Количество видеовыходов (мониторов): 2.
- Разрешение: 1024 × 512.
- Габариты: 44 × 216 × 311.
- Вес: 1.80 кг.
- Вход видеомагнитофона: есть.
- Генератор времени и даты: есть.
- Титры: 8 знаков.
- Экранное меню: есть.
- Zoom: 2-кратный.
- «Alarm» входы: 4, NC или NO.

Мультиплексор MPX-9004E

- Производитель: Appro (Тайвань).
- Цветность: цветной.
- Тип: дуплексный.
- Количество камер: 4.
- Количество мониторов: 1.
- Вес: 3,54 кг.
- Детектор движения: есть.

Видеопринтер P-91E

- Производитель: Mitshubishi (Япония).
- Цветность: черно-белый, 256 градаций серого.
- Разрешение: 1214×600 тчк.
- Плотность печати: 12 тчк/мм (разрешение 300 dpi).
- Размер снимка: 100×75 мм (нормальный формат), 131×99 мм (широкий формат).

§ 3. Средства непосредственного наблюдения

Средства непосредственного наблюдения предназначены для ориентации на местности, визуального наблюдения удаленных предметов и точной наводки огнестрельного оружия в любое время суток.

Приборы наблюдения принято делить на оптические приборы и приборы видения в темноте. Оптические приборы — различного вида бинокли и подзорные трубы — предназначены для наблюдения за удаленными объектами; приборы видения в темноте — за объектами и действиями людей в темное время суток.

Приборы видения в темноте работают по принципу усиления волн инфракрасного диапазона и преобразования их в видимое изображение в электронно-оптическом преобразователе (ЭОП). Инфракрасное излучение может носить естественный характер, например, свет луны и звезд, удаленных фонарей и т. д., либо излучаться самим прибором. Дальность наблюдения зависит от характера наблюдаемых объектов, степени освещенности, контраста между фоном и объектом, прозрачностью атмосферы и ряда других факторов. По наличию или отсутствию собственного источника освещения различают пассивные и активные приборы видения в темноте.

С помощью пассивных приборов возможно наблюдение только при небольшом естественном освещении. Как правило, такие приборы имеют относительно большую дальность за счет применения оптических систем с высоким увеличением. Это такие приборы как ***«Байгыш-6», «Байгыш-12», «Ворон-03».***

Активные приборы позволяют вести наблюдение в абсолютной темноте, например, при обследовании конструктивных пустот зданий и сооружений. Дальность наблюдения таких приборов определяется дальностью источника инфракрасного осветителя. К приборам такого типа относятся ***«Байгыш-19», «Байгыш-20», «Титан-720».*** Средства непосредственно наблюдения делятся на четыре основных вида:

- бинокли;
- ночные бинокли;
- оптические прицелы;
- ночные прицелы.

Бинокли. Бинокли предназначены для ориентации на местности и наблюдения удаленных предметов. Выпускается большое количество разнообразных моделей биноклей. В условные обозначения модели бинокля входят: обозначение типа и исполнение, увеличение и диаметр выходного зрачка. Типы биноклей установлены в зависимости от устройства их оптической схемы. Буква «Б» обозначает соответственно бинокль, «П» — призменные с оборачивающей системой Порро, «Ц» — бинокли с центральным фокусировочным устройством, «О» — с удаленным выходным зрачком, «К» — призма с «крышей», «Ф» — с внутренней фокусировкой.

БПО 7×30 — его основной особенностью является сильно удаленный выходной зрачок, что делает удобным применение его вместе с очками. БКФЦ 7×35 очень компактен и имеет приятный внешний вид. БПЦ 20×60 имеет высокое разрешение. Он очень подходит для наблюдения за удаленными объектами при слабом освещении.

Самые популярные широкоугольные бинокли, созданные на базе современных оптических систем. Предназначены для специалистов и любителей. Отличительные особенности по сравнению с обычными биноклями:

- значительно увеличенное поле зрения;
- улучшенные оптические характеристики и отчетливое изображение не только в центре, но и на краях поля зрения;
- легко находится нужный объект и просматривается широкая панорама на местности.

Бинокли работоспособны при температуре окружающей среды от –30 до +45 °С. Водонепроницаемы при дожде.

В таблице 2.3.1 приведены технико-технические характеристики некоторых биноклей.

Приборы ночного видения являются разновидностью более широкого класса устройств — приборов наблюдения. Известно, что более 90 % сведений об окру-

Таблица 2.3.1 — Технико-технические характеристики биноклей

Модель	БПШЦ 6×30	БПШЦ 7×35	БПШЦ 8×40	БПШЦ 10×50	БПОс 7×30	БКФЦ 7×35М	БПЦ 20×60	БПЦс 8×30	БОЦ 7×50
Увеличение, крат	6	7	8	10	7	7	20	8	7
Угловое поле зрения, не менее, град.	12,30	11	9,3	7,48	8,5	8,5	3,6	8,5	7
Диаметр светового отверстия, мм	30	35	40	50	30	35	60	30	50
Диаметр выходного зрачка, мм	5	5	5	5	4,3	5	3	3,75	7,14
Удаление выходного зрачка	17,5	17,5	17	16,5	22,5	10,5	11	12	21,8
Предел разрешен, угл. сек.	8	6	5	4	7	7,7	3	6	6
Габаритные размеры, мм	173 × 115 × 66	173 × 125 × 60	178 × 145 × 60	188 × 185 × 60	175 × 184 × 63	156 × 120 × 47	260 × 215 × 75	155 × 120 × 60	205 × 191 × 70
Масса, не более, кг	0,65	0,78	0,88	1,00	1,1	0,52	1,40	0,62	0,62

жающем мире человек получает через органы зрения, а дополнительное использование специальных технических средств способствует расширению возможностей выявления и фиксации визуальной информации. Поэтому в практике рассматриваемая группа приборов активно используется при организации наблюдения за встречей подозреваемых лиц, фактами передачи предметов, а также погрузки, выгрузки, выноса похищенных товаров или предметов и др.

По принципу действия приборы наблюдения можно разделить на четыре класса:

– оптико-механические;
– оптические эндоскопы;
– телевизионные;
– электронно-оптические.

Оптико-механические приборы предназначены для наблюдения за объектом на расстоянии или из-за укрытий в дневное и вечернее время суток. Эти приборы объединены в следующие группы:

– бинокли, монокуляры, зрительные трубы, телескопы, специальные объективы, оптические прицелы. Их особенностью является увеличение масштаба изображения контролируемого объекта, что позволяет в процессе наблюдения эффективно использовать их удаленность в качестве основного фактора маскировки;

– устройства, выполненные по перископической схеме, позволяющие полностью замаскировать наблюдателя в укрытии;

– инверторы дверного глазка, дополняющие стандартный глазок и дающие возможность осмотра внутреннего помещения;

– полупрозрачные зеркала, предназначенные для одностороннего наблюдения за объектом на удалении. К ним можно отнести такие отечественные объективы, как «Пеленг», «МТО-500», «МТО-1000», «Таир-3», а также зарубежные объективы фирм Panasonic, Sanyo и др.

Оптические эндоскопы являются средством визуального контроля объектов окружающего пространства и труднодоступных мест (полостей и коммуникаций, внутренних поверхностей корпусов и различных блоков), где невозможен прямой обзор. Эндоскоп представляет собой оптическую систему, состоящую из объектива, системы переноса изображения и окуляра. Рабочей частью устройства являются объектив (совокупность линз) и система переноса изображения (стекловолоконный световод или система зеркал и призм), заключенные в гибкую или жесткую оболочку. Кроме этого в состав эндоскопа входят: наглазник, дистальный (наиболее удаленный) конец световода и ручки управления дистальным концом. В некоторых устройствах предусматривается наличие блока подсветки, что дополнительно расширяет его тактические возможности.

Эндоскопы положительно зарекомендовали себя также и при организации визуального контроля скрытых полостей различных транспортных средств (бензобак, двери, лонжероны и т. д.).

И, наконец, **электронно-оптические приборы** применяются для наблюдения в помещениях или на местности в ночное и вечернее время. В условиях темноты эти приборы позволяют различать силуэты человека, проводить опознание лица по внешним признакам (рост, особенности походки, телосложение), установить номерной знак автомобиля и т. д. Это стало возможным благодаря появлению нового класса приборов — приборов видения в темноте (ПВТ), основным элементом которых является наличие встроенного электронно-оптического преобразователя (ЭОП).

Действие такого ЭОП основано на использовании отраженного от объекта наблюдения изображения в инфракрасном (ИК) диапазоне частот и преобразовании

его сначала в электрический ток с последующим усилением и затем в видимое изображение на экране. В результате такого двойного преобразования картинка получается несколько размытой и это надо учитывать при выборе прибора в каждой конкретной ситуации.

Согласно принятой классификации все **приборы видения в темноте** делятся на два вида: активные и пассивные.

Основным элементом в тех и других приборах является электронно-оптический преобразователь. Разница заключается только в том, что в пассивных приборах источником ИК-излучения является естественное освещение (звезды, луна и т. п.), а активный прибор имеет собственный источник ИК-подсветки. Эта увеличивает мощность падающего на фотокатод светового потока, отраженного от объекта, увеличивает четкость изображения, а значит, появляется возможность наблюдения за удаленными объектами как в вечернее время, так и в условиях полной темноты.

ИК-осветители, используемые в активных приборах видения в темноте, бывают следующих видов:

- электрические лампы накаливания с ИК-светофильтром;
- ИК-светодиоды;
- полупроводниковые ИК-лазеры.

В качестве примера рассмотрим ***прибор ночного видения «МУ-312 8»***, предназначенный для ведения наблюдения в условиях низкой освещенности в ночное время суток. Он оснащен лазерной подсветкой, что позволяет производить наблюдения в условиях полной темноты. Достоинством прибора является отсутствие влияния на качество изображения дисторсии и наличие нелинейной усилительной характеристики. Имеется возможность регулировки размера пятна лазерной подсветки. Прибор комплектуется фотоаппаратом и может быть использован для проведения фото-документирования.

Кроме положительных качеств (работа в условиях полной темноты и низкой освещенности), активные приборы имеют существенный недостаток — возможность его обнаружения наблюдаемой стороной. Пассивный прибор видения в темноте лишен такого недостатка. Не имея собственного источника света, он усиливает с помощью электроники свет Луны, звездный свет или свечение ночного неба до такого уровня, при котором наблюдаемая через телескоп картинка получается достаточно четкой и яркой.

Представляет значительный интерес ***серия приборов ночного видения «Ворон».*** Они предназначены не только для наблюдения, но и фотовидеорегистрации изображений объектов в вечернее и ночное время в полевых условиях, на городских улицах и в затемненных помещениях. Модификация приборов различается по комплектации, в которую могут входить телепереходник для ТВ-камеры типа «Электроника», фотопереходник для фотокамеры типа «Зенит», миниатюрная телевизионная установка МТУ-1 с блоком синхронизации и ТВ-адаптер для записи на видеомагнитофон. Блок синхронизации предназначен для согласования работы МТУ-1 с видеомагнитофоном при осуществлении записи визуальной информации. При комплектовании прибора инфракрасным лазерным осветителем «Выпь» обеспечивается подсветка объективов приборов ночного видения «Ворон-1», «Ворон-2», «Ворон-3». В результате они становятся активными, что обеспечивает наблюдение за объектом в условиях полной темноты. В ИК-осветителе «Выпь» предусмотрены два режима работы: продолжительный (при запуске от встроенного переключателя) и импульсный (при запуске от синхроконтакта фотоаппарата).

Прибор ночного видения НН-12 предназначен для прицеливания при стрельбе и наблюдения за полем боя. Дальность видения целей зависит от величины естественной освещенности, прозрачности атмосферы и контраста между фоном и целью.

Естественная ночная освещенность может изменяться в довольно широких пределах и составляет в ясную лунную ночь — 0,2 лк; в ясную безлунную ночь — 0,001 лк. В самые темные ночи (в пасмурную погоду) освещенность может снижаться до 0,0001 лк. При освещенности больше 0,003–0,005 лк, если цель рассматривается на светлом фоне (песок, снег и т. п.) дальность видения увеличивается. Она увеличивается также при наблюдении за движущимися объектами. При освещении ниже 0,003 лк при низкой прозрачности атмосферы, а также если наблюдаемый объект рассматривается на темном фоне (хвойный лес, пашня и т. д.), дальность видения уменьшается. При освещенности 0,005 лк фигура человека различается на расстоянии 400–500 м.

Технические характеристики:

Увеличение	4,5х
Угол поля зрения	4030'
Фокусное расстояние, мм	118
Относительное отверстие объектива	1 : 1,55
Напряжение питания, В	3,75
Габаритные размеры, мм	535 × 150 × 130
Источник питания	аккумуляторная батарея
Масса источника, питания, кг	3,3
Время непрерывной работы без замены источников питания (при температуре окружающей среды 20 °С), ч	не менее 6

В комплект прибора входят: большая и малая тренога, переносная сумка, чехол.

К приборам этого же класса относится ***ночной стрелковый прибор НСП-3,*** предназначенный для прицеливания при стрельбе из автомата АКМЛ, ручного пулемета РПКЛ и наблюдение за полем боя.

Дальность прицеливания стрельбы из автомата АКМЛ и ручного пулемета РПКЛ с ночным стрелковом приборов НПС-3 по фигуре солдата в полный рост в защитном обмундировании в безлунную звездную ночь в средних широтах при естественной освещенности 0,003–0,005 лк составляет 250–300 м.

Под дальностью прицельной стрельбы понимается дальность видения цели, при которой можно вести по ней стрельбу.

Технические характеристики:

Дальность видения фигуры в полный рост, м	250–300
Увеличение	2,7х
Угол поля зрения	7°
Фокусное расстояние объектива, мм	78
Питание	аккумуляторная батарея ЗСЦС-1,5
Напряжение питания, В	4,5
Потребляемый ток, А	0,2
Масса прицела, с источником питания, кг	2,7
Габаритные размеры прицела, мм	450 × 105 × 175

Действие прицела основано на принципе электронно-оптического усиления яркости изображения предметов (целей) полученного в прицеле при естественной ночной освещенности на местности. Наблюдение при естественной ночной освещенности можно осуществлять при помощи электронно-оптического прибора, состоящего из объектива, дающего изображение наблюдаемого объекта, электронно-оптического преобразователя, усиливающего яркость этого изображения, и окуляра для рассматривания изображения, получаемого на экране ЭОП. Изображение местности и цели, наблюдаемое в прицел, имеет желто-зеленый цвет свечения люминофора на экране ЭОП. Конструктивно прицел состоит из следующих частей:

– объектива с механизмом светофильтров, который выполнен в виде двух блоков, состоит из пяти линз и содержит три светофильтра (нейтральный НС-8, красный КС-17, желтый ЖС-18) для повышения контраста изображения;

– механизма выверок прицела по направлению и высоте, а также для введения углов прицеливания;

– трехкаскадного ЭОП в подвеске;

– делителя напряжения для подачи напряжения на каждую камеру (каскад) ЭОП;

– преобразователя напряжения постоянного тока в высокое напряжение переменного тока;

– высоковольтного блока для преобразования переменного напряжения в высокое напряжение постоянного тока, необходимого для питания ЭОП;

– окуляра с корпусом для увеличения изображения, получаемого на экране ЭОП;

– аккумуляторной батареи;

– корпуса прицела с зажимным устройством для осуществления крепления прицела на оружии.

Ночные бинокли. Ночные бинокли предназначены для ориентации на местности и наблюдения удаленных предметов в темное время суток.

«Филин-1». Ночной бинокль «Филин 1» является оптико-электронным прибором, предназначенным для визуального наблюдения объектов в темное время суток, ориентирования на местности, на водной поверхности в условиях естественной ночной освещенности. Принцип работы ночного бинокля основан на преобразовании невидимых глазом инфракрасных лучей, отраженных от объектов, в видимое изображение с помощью электронно-оптического преобразователя. Для работы в условиях низкой освещенности в бинокле предусмотрен инфракрасный осветитель (ИК-светодиод).

«Филин-1» выпускается следующих модификаций:

БНО 1×39; БНО 1,7×48; БНО 2,5×42; БНО 2,5×48; БНО 2,5×56; БНО 4×48; БНО 5,5×56; БНО 7×70.

БАЙГЫШ-7С. Байгыш-7С является сложным оптоэлектронным устройством ночного видения, предназначенным для ночного наблюдения и ориентации на местности ночью при слабом освещении. Устройство объединяет в себе три функции:

- адаптирован для камер (может использоваться для обзора и фотографирования при очень слабом освещении);
- имеет бинокулярный окуляр (для удобного обзора обоими глазами);
- имеет монокулярный окуляр (позволяет получить более сильное увеличение).

Циклоп 102. Ночной бинокль второго поколения Циклоп 102 предназначен для рассматривания и ориентации на местности в условиях естественной ночной или слабой искусственной освещенности.

БНВ-2. Бинокль ночного видения является оптико-электронным прибором, предназначенным для визуального наблюдения объектов в ночное время суток, ориентирования на местности, на водной поверхности при естественной освещенности от 5×10^{-8} до 1 лк и более низких уровнях освещенности с использованием встроенного ИК-осветителя.

БНВ 2,5×42. Бинокль ночного видения Сибирь БНВ 2,5×42 это прибор профессионального качества, предназначенный для высококачественного обзора вблизи в полной темноте. БНВ 2,5×42 пассивный прибор: он не требует никаких дополнительных источников света, хотя источник инфракрасного света сильно увеличивает эффективность наблюдения.

БНВ 2,5×42 сконструирован из 2 двух отдельных электронно-оптических блоков, установленных в обрезиненный корпус из водостойкого пластика. Наружная

Таблица 2.3.2 — Основные технико-технические характеристики ночных биноклей

Модель	ФИЛИН 1	БАЙ-ГЫШ-7С	ЦИКЛОП 102	БНВ-2	БНВ 2,5 × 42
Увеличение, крат	4	4,3	4,5	2,0	2,5
Угловое поле зрения, не менее, град	9	7	8	21°30'	18°
Пределы перефокусировки окуляров, дптр	от +5 до –5	от +4 до –4	от +4 до –4	от +4 до –4	от 5 до –5
Напряжение питания номинальное, В	3	9	3	3	1,5
Время непрерывной работы, час	6	5	8	6	20
Габаритные размеры, мм	215 × 140 × 90	318 × 173 × 84	300 × 130 × 80	137 × 220 × 67	165 × 160 × 76
Масса, не более, кг	1,16	1,7	1,0	1,0	0,8

поверхность прибора шероховатая, негладкая для экстремальных полевых условий. Однако при небрежном эксплуатировании может выйти из строя. Прибор полностью автономен и может действовать на двух АА-батареях.

В таблице 2.3.2 приведены основные технико-технические характеристики перечисленных ночных биноклей.

Оптические прицелы. Оптические прицелы предназначены для точной наводки при стрельбе. Оптические прицелы уменьшают утомление глаз вследствие того, что мишень увеличена, а также из-за отсутствия параллакса.

ПОСП 4 × 24

Увеличение, крат	4
Угловое поле зрения, не менее, град.	4
Диаметр выходного зрачка, мм	4
Диаметр линз, мм	24
Длина, мм	337
Масса, не более, кг	0,62

ПОСП 6 × 24

Увеличение, крат	6
Угловое поле зрения, не менее, град.	4
Диаметр выходного зрачка, мм	4
Диаметр посадочный, мм	12
Диаметр линз, мм	24
Длина, мм	337
Масса, не более, кг	0,62

ПОСП 6 × 42

Увеличение, крат	6
Угловое поле зрения, не менее, град.	4
Диаметр выходного зрачка, мм	6,7
Диаметр линз, мм	42
Длина, мм	406
Масса, не более, кг	0,75

ПО 4×24

Увеличение, крат	4
Угловое поле зрения, не менее, град.	6
Диаметр выходного зрачка, мм	8
Диаметр посадочный, мм	25,4
Диаметр линз, мм	24
Длина, мм	255
Масса, не более, кг	0,30

ПИЛАД 8×56, 8×56L

В отличие от предыдущей модели, Р8×56L имеет подсветку прицельной метки, что облегчает прицеливание в сумерках. Технические характеристики приборов идентичны.

Р8×56

Р8×56L

Увеличение, крат	8
Угловое поле зрения, не менее, град.	3,20
Диаметр выходного зрачка, мм	8
Диаметр посадочный, мм	26
Диаметр линз, мм	56
Длина, мм	307
Масса, не более, кг	0,45

ПС 4×43

Увеличение, крат	4
Угловое поле зрения, не менее, град.	6
Диаметр выходного зрачка, мм	10,6
Диаметр посадочный, мм	25,4
Диаметр линз, мм	52
Длина, мм	281
Масса, не более, кг	0,42

Ночные прицелы.

Байгыш-5П. Прицел ночного видения Байгыш-5П предназначен для стрельбы при естественном ночном освещении. Прицел может быть укомплектован инфракрасным осветителем для улучшения качества изображения при недостаточном освещении.

Увеличение, крат	2,5 ± 0,3
Угловое поле зрения, не менее, град.	7
Пределы перефокусировки окуляров, дптр.	от +3 до –3
Дальность обнаружения цели, м	400
Напряжение питания номинальное, В	9
Габаритные размеры, мм	
– без подсветки	420 × 105 × 70
– с подсветкой	420 × 145 × 70
Масса прицела, не более, кг	1,5
Масса прицела с подсветкой	1,8

НП-75

Ночной прицел НП-75 предназначен для прицельной наводки на цель при стрельбе в сумерках и ночью. При использовании прицела днем наблюдение производится через точечное отверстие в крышке объектива. Для наведения на цель служит светящаяся прицельная марка в поле зрения прицела. Плавная регулировка яркости марки позволяет производить прицеливание на цели с различной освещенностью.

Увеличение, крат	2
Угловое поле зрения, не менее, град.	12
Пределы перефокусировки окуляров, дптр.	от +4 до –4
Дальность обнаружения цели, м	400
Напряжение питания номинальное, В	3
Габаритные размеры, мм	256 × 72 × 76
Масса прицела, не более, кг	0,95

PNS 2,4 × 30

Увеличение, крат	2,2
Угловое поле зрения, не менее, град.	12
Пределы перефокусировки окуляров, дптр.	от +3 до –3
Дальность обнаружения цели, м	200
Напряжение питания номинальное, В	9
Габаритные размеры, мм	164 × 50 × 102
Масса прицела, не более, кг	0,6

PNS 4,6 × 52

Увеличение, крат	4,6
Угловое поле зрения, не менее, град.	6
Пределы перефокусировки окуляров, дптр.	от +3 до –3
Дальность обнаружения цели, м	200
Напряжение питания номинальное, В	9
Габаритные размеры, мм	214 × 59 × 102
Масса прицела, не более, кг	0,85

Тема 3. СРЕДСТВА ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Техническое средство охраны — это базовое понятие, обозначающее аппаратуру, используемую в составе комплексов технических средств, применяемых для охраны объектов от несанкционированного проникновения.

Техническое средство охраны — это вид техники, предназначенный для использования силами охраны с целью повышения эффективности обнаружения нарушителя и обеспечения контроля доступа на объект охраны.

Каждое средство охраны строится на определенном физическом принципе, на основе которого действует его чувствительный элемент. Таким образом:

– *чувствительный элемент* — это первичный преобразователь, реагирующий на воздействие на него объекта обнаружения и воспринимающий изменение состояния окружающей среды;

– *средство обнаружения (СО)* — это устройство, предназначенное для автоматического формирования сигнала с заданными параметрами вследствие вторжения или преодоления объектом обнаружения чувствительной зоны данного устройства.

§ 1. Особенности построения и тенденции развития современных технических средств охранной сигнализации

Решение задач обеспечения безопасности объектов все в большей мере опирается на широкое применение технических средств охранной сигнализации (ТСОС). При выборе и внедрении ТСОС на объектах уделяется особое внимание достижению высокой защищенности аппаратуры от ее преодоления. Производители ТСОС предлагают различные способы реализации этой задачи: контроль вскрытия блоков, автоматическая проверка исправности средств обнаружения и каналов передачи информации, защита доступа к управлению аппаратурой с помощью кодов, архивирование всех возникающих событий, защита информационных потоков между составными частями ТСОС методами маскирования и шифрования и др. Как правило, современные ТСОС имеют одновременно несколько степеней защиты.

Таким образом, одной из главных задач при проектировании ТСОС является создание средств защиты от обхода их злоумышленником и это является сложнейшей многоплановой задачей.

Системы охранной сигнализации фиксируют факт несанкционированного доступа на охраняемую территорию, передают сигнал тревоги, например, на пульт охраны и включают исполняющие устройства.

Включают:

– датчики;

– пульт-концентратор;

– исполняющие устройства.

Датчик — чувствительный элемент, преобразующий контролируемый параметр в электрический сигнал.

Особенность датчиков для систем охранной сигнализации состоит в том, что они регистрируют, в основном, неэлектрические величины. Измерение неэлектрических величин — сложная задача и при этом датчики должны обеспечивать высокую надежность и достоверность контроля. Надежность датчиков обеспечивает-

ся, в основном, цифровыми методами обработки сигналов. Датчики объединяются в зоны. Под зоной понимается один или несколько датчиков, охраняющих определенный объект или участок объекта.

Пульт-концентратор — центральное устройство системы охранной сигнализации. Он выполняется на базе микропроцессора. Все функции системы определяются программой микропроцессора. Параметры программы задает пользователь, в зависимости от его полномочий, со специального пульта. Пульты-концентраторы могут подключаться к персональным ЭВМ для обработки и регистрации сигналов тревоги, автоматического анализа состояния датчиков и функционирования всей системы. Пульты-концентраторы могут принимать и передавать сообщения по телефонной сети через коммуникационный модуль в автоматическом режиме.

Большинство систем охранной сигнализации дополняются датчиками пожарной безопасности. Наиболее развитые системы могут включать другие подсистемы и дополняться, например, пультами дистанционного управления.

По способу подключения датчиков к пультам-концентраторам охранные устройства разделяются на проводные и беспроводные.

В проводных системах связь между всеми устройствами системы осуществляется по кабелю. При высокой надежности проводных систем они менее гибкие, чем беспроводные.

В беспроводных системах каждый датчик оснащается собственным передатчиком, а пульт-концентратор — многоканальным приемником. Приемник и передатчик могут быть встроенными, либо выполненными в виде отдельных модулей. Беспроводные системы охранной сигнализации более удобны при монтаже и использовании. Они могут дополняться сервисными устройствами дистанционного управления.

Очевидно, создание программно-аппаратных средств защиты ТСОС от обхода невозможно без глубоких и исчерпывающих знаний о структуре построения, функциональных возможностях и принципах работы ТСОС.

Динамика мирового развития ТСОС диктует необходимость изучения структурного и функционального построения не только современных ТСОС, но и отслеживание тенденций развития аппаратуры в перспективе. Такой мониторинг позволяет проводить упреждающие разработки ТСОС, аналоги которых ожидаются к появлению в ближайшее время.

Технические средства охранной сигнализации входят в состав комплекса технических средств охраны наряду с техническими средствами наблюдения, средствами управления доступом и вспомогательными средствами, объединенными общей оперативно-тактической задачей. Как правило, это автоматизированные системы охраны.

В свою очередь комплекс ТСОС в совокупности с инженерными средствами охраны, объединенные для решения общей задачи по охране объекта, образуют законченный комплекс инженерно-технических средств охраны.

Под **комплексом ТСОС** понимается совокупность функционально связанных средств обнаружения, системы сбора и обработки информации и вспомогательных средств и систем, объединенных задачей по обнаружению нарушителя.

Под **системой сбора и обработки информации (ССОИ)** понимается совокупность аппаратно-программных средств, предназначенных для сбора, обработки, регистрации, передачи и представления оператору информации от средств обнаружения, для управления дистанционно управляемыми устройствами, а также для контроля работоспособности как средств обнаружения, дистанционно управляемых

устройств и каналов передачи, так и работоспособности собственных составных элементов.

Аппаратура ССОИ подразделяется на:

– станционную, осуществляющую прием, обработку, отображение и регистрацию информации, поступающей от периферийной аппаратуры ССОИ, а также формирование команд управления и контроля работоспособности;

– периферийную, осуществляющую прием информации от средств обнаружения, ее предварительную обработку и передачу ее по каналу передачи на центральную станционную аппаратуру, а также прием и передачу команд управления и контроля работоспособности.

Структура типовых вариантов построения комплексов ТСОС определяется распределением логической обработки информации от средства обнаружения (СО) между станционной аппаратурой и периферийными блоками, а также способом связи между ними и средством обнаружения. На выбор варианта структуры построения комплекса главным образом оказывают влияние следующие факторы:

– качественный и количественный состав обслуживаемых СО и ПБ;
– степень централизации управления ССОИ;
– структурные особенности охраняемых объектов;
– стоимостные и надежностные факторы.

Известны следующие основные способы соединения станционной аппаратуры с периферийными блоками и СО:

1. *Радиальный бесконцентраторный* (рис. 3.1.1).

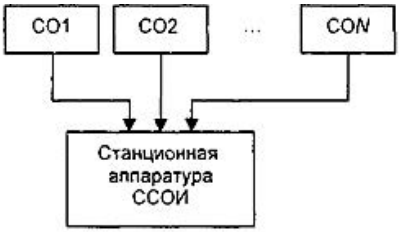


Рисунок 3.1.1 — Радиальное (лучевое) бесконцентраторное соединение станционной аппаратуры с СО

Как правило, комплексы ТСОС с радиальной бесконцентраторной структурой имеют следующие основные особенности:

– простота исполнения и технического обслуживания аппаратной части;

– подключение каждого СО осуществляется по отдельным цепям электропитания, дистанционной проверки и контроля состояния;

– неисправности, возникающие в линиях связи СО и входных цепях станционной аппаратуры, влияют на работоспособность только отдельного канала сигнализации, что при соответствующей организации охраны не влияет на функционирование всего комплекса ТСОС;

– значительный объем и разветвленность кабельных линий.

2. *Радиальный с концентраторами* (рис. 3.1.2). Назначение концентраторов в ССОИ разного типа может отличаться по различным признакам. Кроме функций *увеличения емкости аппаратуры и уплотнения передаваемой информации* концентраторы могут служить для объединения средств обнаружения по участкам блоки-

рования, автоматической проверки их работоспособности и обеспечения контроля линии связи.

В отдельных системах кроме названных функций в концентраторы закладываются функции предварительной обработки сигналов от средств обнаружения. Через них же осуществляется и электропитание средств охраны.

Рисунок 3.1.2 — Радиальное (лучевое) с концентраторами соединение станционной аппаратуры с ПБ и СО

К особенностям комплексов ТСОС с радиальной структурой с концентраторами можно отнести следующие:

– при постановке на охрану/снятии с охраны какого-либо канала сигнализации подача/снятие электропитания осуществляется на всю группу каналов, подключенных к одному концентратору, т. е. по одной линии связи осуществляется электропитание концентратора и всех средств обнаружения, подключенных к данному концентратору. Это обстоятельство можно не учитывать при малом энергопотреблении СО и малых расстояниях от СО до станционной аппаратуры, однако оно накладывает жесткие ограничения на сопротивление соответствующих соединительных проводов при значительном энергопотреблении или при большой длине линии связи;

– более высокая стоимость аппаратуры по сравнению с аппаратурой комплексов, построенных по радиальной бесконцентраторной схеме;

– при нарушении связи с концентратором теряется информация о состоянии целой группы СО, подключенной к нему.

Основное достоинство комплексов с такой структурой — относительно низкая стоимость кабельных коммуникаций и относительно короткое время их монтажа.

3. *Шлейфовый без концентраторов и с концентраторами* (рис. 3.1.3–3.1.4).

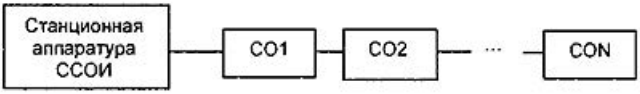


Рисунок 3.1.3 — Шлейфовое (магистральное) без концентраторов соединение станционной аппаратуры с СО

Работоспособность комплексов ТСОС с шлейфовой структурой в большой степени определяется исправным состоянием линий связи, поскольку возникновение короткого замыкания в линии полностью нарушает работу комплекса, а в случае

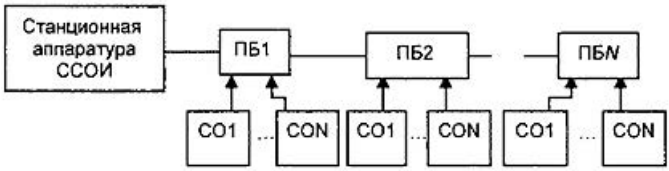


Рисунок 3.1.4 — Шлейфовое (магистральное) с концентраторами соединение станционной аппаратуры с ПБ и СО

обрыва в рабочем состоянии остается только та часть комплекса, с которой поддерживается связь. Учитывая данное обстоятельство, в последнее время используется резервирование соединительных линий и узлов. При этом подача электропитания и связь с устройствами комплекса осуществляется по двум независимым шлейфам. Поэтому при выходе из строя одного из них работоспособность комплекса поддерживается за счет другого. Однако в этом случае стоимость кабельных линий и электромонтажных работ увеличивается практически в два раза. Также на работоспособность комплекса ТСОС со шлейфовой структурой большое влияние оказывает организация электропитания СО, так как питание должно подаваться по ограниченному количеству проводов и должен учитываться суммарный ток потребления всех СО и концентраторов.

4. *Смешанная или древовидная структура* (рис. 3.1.5).

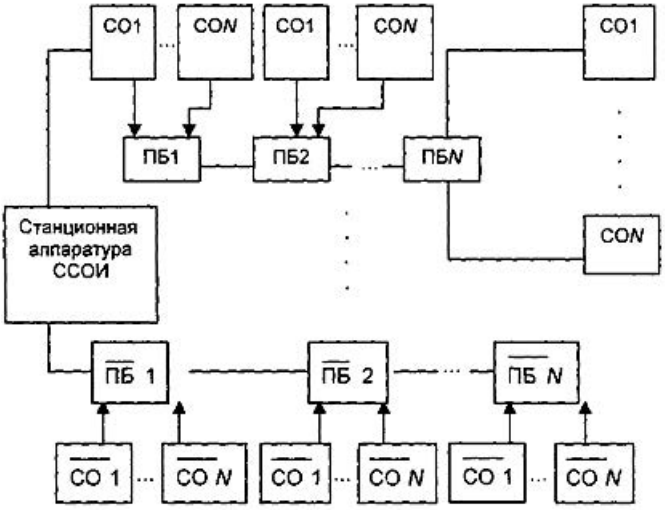


Рисунок 3.1.5 — Смешанное (радиально-шлейфовое) соединение станционной аппаратуры с ПБ и СО

Данная структура системы сбора и обработки информации является комбинацией технических средств, соединенных по радиальной и шлейфовой схемам.

Необходимо отметить, что указанные способы связи периферийных блоков и средств охраны со станционной частью ССОИ могут быть использованы и для

организации связи СО с ПБ. Связь ПБ с СО также может быть организована посредством локальной сети, имеющей шлейфовую или древовидную структуру.

Для включения средств охраны на общую магистраль локальной сети необходима разработка специальных блоков сопряжения, устанавливаемых рядом с каждым СО и служащих буфером между сетью и стандартизованными выходными/входными цепями СО в виде контактов реле. Однако, зачастую стоимость такого устройства может быть соизмерима со стоимостью некоторых СО и будет превышать выигрыш в стоимости, получаемый за счет сокращения длины кабелей связи.

При выборе структуры построения комплекса ТСОС и соответствующей аппаратуры ССОИ учитываются:

– категория объекта, оснащаемого комплексом;
– затраты на оборудование объекта;
– уровень подготовленности персонала, которому предстоит работать с устанавливаемым комплексом;
– время поиска и устранения неисправностей и надежность линии связи.

Для комплексов относительно небольшой емкости, как правило, используется радиальная схема соединения периферийных устройств и средств обнаружения со станционной аппаратурой, а для комплексов большей емкости — шлейфовая с концентраторами сигнализационной информации. При этом обработка информации должна осуществляться преимущественно в концентраторах, объединенных со станционной частью по шинной структуре.

Как правило, наиболее предпочтительным является смешанная структура построения комплексов ТСОС:

– для наиболее важных участков блокирования — радиальная структура;
– для менее важных помещений — шлейфовая/магистральная структура.

Отличительной особенностью построения комплексов ТСОС, содержащих многие типы средств обнаружения, являются способы адаптации ССОИ к конкретным типам контролируемых ею СО. При сопряжении СО и ССОИ необходимо согласовать следующие стыковочные параметры:

– напряжение электропитания СО;
– время неустойчивого состояния выходных контактов СО после подачи на него напряжения электропитания;
– тип дистанционной проверки работоспособности СО.

В целях осуществления контроля за действиями оператора по управлению комплексом ТСОС и для удобства оперативной работы в состав комплекса вводится аппаратура хранения и документирования информации. Наибольшее распространение получили накопление информации в специальном оперативном запоминающем устройстве или на жестком диске ПЭВМ с возможностью вывода информации на буквенно-цифровой индикатор и ее распечатывания.

Однако введение в состав комплекса устройств документирования требует предусматривать блоки автоматики, предназначенные для логической обработки и подготовки сигналов управления блоками цифро-печатающего устройства. В последнее время для документирования и систематизации сигнализационной информации в состав ССОИ вводится блок стыковки с ПЭВМ. Сигнализационная информация из ОЗУ ССОИ через этот блок передается в ПЭВМ, где ее можно систематизировать:

– по выбранным каналам;
– по выбранному интервалу времени;
– по видам сообщений.

В комплексах ТСОС передача информации между средствами обнаружения, периферийными устройствами и станционной частью ССОИ может осуществляться по линиям связи разного типа. В зависимости от используемого типа линии связи различают следующие комплексы ТСОС:

– с проводными линиями связи;
– с радиоканалами связи;
– с оптоволоконными линиями связи;
– со специальными линиями связи.

В большинстве современных комплексов ТСОС используются проводные линии связи. В качестве проводных линий могут использоваться специально проложенный кабель, телефонные линии — свободные и занятые, электросеть, телевизионные кабели.

В мобильных комплексах, как правило, обеспечивается организация радиолинии связи между блоками ТСОС. Радиоканалы могут использовать разные частоты, виды модуляции и мощности передатчика. Во всех случаях применения радиолинии связи необходима подача автономного электропитания на периферийные блоки, а значит и на средства охраны.

В ближайшее время в связи с непрерывным снижением стоимости услуг и оборудования систем сотовой связи с большой вероятностью можно предположить, что для передачи данных между устройствами комплекса ТСОС все более широко будут использоваться каналы сотовой связи. Но этого может и не произойти, если не будут найдены надежные способы защиты сотовой связи при их использовании в системах безопасности и не будут найдены способы обеспечения надежности такой связи.

Использование сотовых систем связи оправдано в случаях, когда необходимо снизить габариты аппаратуры, уровень собственных электромагнитных излучений, а также когда нужно обеспечить большую площадь действия системы. Параметры канала передачи данных позволяют обеспечить передачу речевой или малокадровой видеоинформации, что позволяет реализовать дополнительные функции обеспечения безопасности.

При организации передачи данных по каналам сотовой связи в системах безопасности стационарных объектов обеспечиваются гибкие алгоритмы опроса датчиков, полная автономность обеспечения работоспособности системы. Диспетчерский центр контролирует работоспособность системы путем периодического опроса состояния датчиков. Сигнал тревоги поступает на пульт с задержкой не более 20 с.

В современных линиях передачи информации находят применение и волоконно-оптические линии связи, построенные на основе волоконных световодов. Они по сравнению с проводными линиями связи обладают рядом преимуществ:

– высокая скрытность передачи данных;
– высокая скорость передачи данных;
– высокая помехозащищенность и нечувствительность к электромагнитному излучению;
– малая масса.

Наиболее дорогими компонентами волоконно-оптических систем по сравнению с электрическими проводными являются разъемы, кабели, коммутаторы, ответвители, переключатели и т. п.

В связи с этим стоимость оптоэлектронных узлов комплексов ТСОС в настоящее время дороже в 3–5 раз их проводных аналогов. Причем, в комплексах с опто-

волоконным каналом обмена данными необходима организация автономного электропитания каждого ПБ и СО.

По указанным причинам в настоящее время оптоволоконные линии связи редко используются в комплексах ТСОС стационарных объектов.

На ряде охраняемых объектов требуется применение комплексов ТСОС с высокой степенью защиты соединительных сигнализационных линий от несанкционированного внедрения. В настоящее время для этих целей, как правило, используются ССОИ, обеспечивающие защиту сигналов, передаваемых по линии связи между средствами охраны и ССОИ.

Часто требуется организация охраны ряда рассредоточенных объектов. В этом случае используется система централизованной охраны, как правило, привязанная к станционной и линейной аппаратуре городской телефонной сети и осуществляемая с помощью систем передачи извещений (СПИ). Посредством СПИ информация передается на диспетчерский пункт централизованной охраны.

Под **системой передачи извещений** понимается совокупность совместно действующих технических средств для передачи извещений о проникновении на охраняемые объекты, служебных и контрольно-диагностических извещений, а также для передачи и приема команд телеуправления.

Структурная схема системы с централизованным наблюдением представлена на рисунке 3.1.6.

Объектовое оконечное устройство — это составная часть СПИ, устанавливаемая на охраняемом объекте для приема извещений от ПКП, преобразования сигналов и их передачу по каналу связи на ретрансляторы, а также для приема команд телеуправления от ретранслятора.

Ретранслятор — это составная часть СПИ, устанавливаемая в промежуточном пункте между охраняемым объектом и ПЦО или на охраняемом объекте для приема извещений от объектовых оконечных устройств или других ретрансляторов, преобразования сигналов и их передачи на последующие ретрансляторы или на ПЦН, а также для приема от пульта или других ретрансляторов и передачи на объектовые оконечные устройства или ретрансляторы команд телеуправления.

Пульт централизованного наблюдения — это самостоятельное техническое средство или составная часть СПИ, устанавливаемая на ПЦО для приема от ретрансляторов извещений, обработки, отображения, регистрации полученной информации, а также для передачи на ретрансляторы и объектовые оконечные устройства команд телеуправления.

По типу используемых линий связи следует выделить СПИ, использующие:

- линии телефонной сети;
- радиоканалы;
- специальные линии связи;
- комбинированные линии связи и др. (рис. 3.1.6).

Можно утверждать, что в ближайшие годы область охранных технологий продолжит свое бурное развитие, продолжится широкое внедрение передовых средств микропроцессорной и вычислительной техники. Благодаря развитию элементной базы все большее применение при построении отдельных устройств и узлов современных комплексов ТСОС будут находить цифровые электрические схемы, особенно на основе микроконтроллеров.

В системе сбора и обработки информации микроконтроллеры позволяют значительно упростить создание схем обработки информации от СО, от элементов, контролирующих состояние системы, от устройств ввода/вывода за счет разработ-

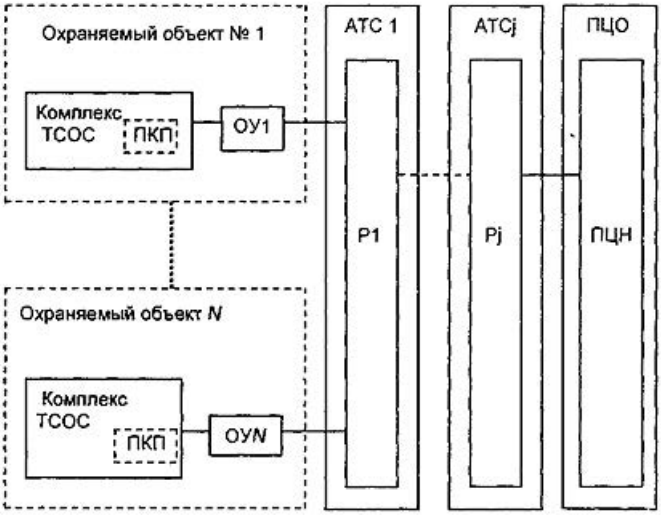


Рисунок 3.1.6 — Структурная схема СПИ с централизованным наблюдением

ки специального программного обеспечения. Это, в конечном итоге, заметно снижает габаритные размеры, стоимость и увеличивает унифицируемость систем, что легче и дешевле переработки принципиальных схем узлов ССОИ.

Применение цифровой элементной базы при построении СО позволяет реализовать более оптимальные алгоритмы обработки сигналов от чувствительных элементов СО, что, в свою очередь, приводит к улучшению тактико-технических характеристик, таких как:

- вероятность обнаружения;
- вероятность ложного срабатывания;
- наработка на ложное срабатывание.

Кроме того, отчетливо проявляются тенденции снижения энергопотребления, излучаемых мощностей, габаритных размеров, стоимости СО, улучшения маскирующих свойств СО.

В перспективе процессы обработки, отображения, хранения и документирования информации, обмена информацией с другими системами будут по-прежнему возложены, в основном, на персональные компьютеры. Применение последних достижений компьютерных технологий позволит создавать интеллектуальные системы охранной сигнализации с высоким уровнем автоматизации. Разработка новых способов отображения вплоть до создания трехмерной графической модели охраняемого объекта, на которой отображены все СО, режимы их работы и состояние, откроет возможность повышения наглядности изображения места проникновения нарушителя и направления его движения. Увеличение объемов сохраняемой информации и новые способы ее обработки позволят создавать автоматизированные базы данных. Управление комплексом технических средств охраны, как правило, будет осуществляться с помощью клавиатуры, манипулятора «мышь», сенсорных экранов.

Таким образом, анализ структурных схем построения и схемотехнических решений отдельных блоков показывает, что в последующие годы технические

средства охранной сигнализации будут развиваться в направлении создания многофункциональных аппаратно-программных центров сбора и обработки информации, поступающей от разных подсистем, т. е. в направлении создания единой интегрированной системы безопасности объекта. ТСОС будут обладать универсальностью и гибкостью структуры, адаптивно настраиваться на решение конкретных тактических задач. ТСОС будут становиться все более «интеллектуальными», будет повышаться уровень их автоматизации: они смогут самостоятельно, практически без участия оператора, формировать ответные реакции на потоки поступающих событий.

Интегрированные системы безопасности будут представлять собой аппаратно-программные комплексы с общей базой данных. В качестве устройств управления будут использоваться компьютерные терминалы со специализированным программным обеспечением.

Благодаря интеграции отдельных подсистем, применению компьютера в качестве устройства контроля и управления и развитию соответствующих компьютерных технологий обработки информации будут достигаться:

– высокий уровень автоматизации процессов управления функционированием технической системы обеспечения безопасности и реагирования на внешние события;

– снижение влияния человеческого фактора на надежность функционирования системы;

– взаимодействие аппаратуры разного назначения, исключающее противоречивые команды благодаря организации гибкой системы внутренних приоритетов и/или их адаптивной настройки на происходящие в системе события;

– упрощение процесса управления со стороны оператора интегрированной системой безопасности;

– более высокий уровень разграничения прав доступа к информации;

– повышение степени защиты от несанкционированного доступа к управлению;

– общее снижение затрат на создание ИСБ за счет исключения дублирующей аппаратуры;

– повышение эффективности работы каждой из подсистем и реализация ряда других свойств.

§ 2. Классификация чувствительных элементов средств обнаружения

При своем движении человек-нарушитель оставляет множество разнообразных следов своего движения и пребывания, которые могут быть зафиксированы различными приборами. На самом деле, человек обладает вполне определенными параметрами, как то: геометрическими размерами, массой, температурой тела, запахом, электрическими, биомеханическими и биодинамическими характеристиками, скоростями движения, частотой шага и т. д.

При своем движении он возбуждает звуковые и ультразвуковые колебания в атмосфере и окружающих предметах, а также сейсмические колебания в почве и строительных конструкциях. В процессе выполнения тех или иных действий человек оказывает непосредственное силовое воздействие на интересующие его предметы, а также динамическое воздействие на поля электромагнитной и акустической энергии, вызывая нарушения их структуры в пространстве.

Движение человека сопровождается генерацией сверх низкочастотных электрических полей, возникающих как следствие переноса индуцированного в результате трения обуви о поверхность пола и взаимного трения элементов тела и одежды электростатического заряда.

Кроме того, известно, что в процессе физической деятельности человек излучает электромагнитные сигналы в очень широком спектре частот, а органы дыхания и кровообращения генерируют акустические колебания. Потовые железы человека выделяют в окружающую атмосферу продукты, в составе которых насчитываются десятки химических веществ, некоторые из которых являются характерными только для человека.

В процессе проникновения в помещение нарушитель открывает двери, окна, форточки; иногда вынужден вырезать и/или выбивать стекла, либо проделывать отверстия и проломы в потолках, полу или стенах. Внутри помещения он передвигает предметы, обстановку, пытается вскрыть металлические шкафы или сейфы, фотографировать документы или изделия. Для выполнения этих действий он может иметь с собой фотоаппаратуру, различный инструмент, а также оружие или взрывчатые вещества. Указанные факторы обладают самостоятельными информативными характеристиками, обнаруживающими присутствие человека в охраняемом помещении, одновременно увеличивая объем информации о нем.

Так, имеющееся у нарушителя оружие или инструмент обладают определенными физическими параметрами, и их наличие может привести к изменению напряженности магнитного поля, частоты облучающего СВЧ сигнала. Применение механического инструмента для открывания дверей и металлических шкафов, образование проломов и отверстий в стенах и полах помещений сопровождается возбуждением характерных колебаний в твердых телах и акустических волн в воздушной среде помещения.

При использовании газовой горелки имеет место тепловое излучение пламени, изменяется температура подвергающегося воздействию нарушителя объекта, появляется специфический запах горючей смеси, который, как и в случае применения взрывчатых веществ, приводит к изменению химического состава воздуха.

Таким образом, появление нарушителя на охраняемой территории в общем случае может быть обнаружено по большому числу физико-химических явлений. Это обнаружение осуществляется с помощью технических средств, в основу построения которых положены самые различные принципы регистрации изменений состояния среды.

Основные типы чувствительных элементов, осуществляющих взаимодействие с внешней средой и нарушителем, которые могут быть положены в основу построения соответствующих типов средств охраны, приведены на рисунке 3.2.1.

Схема, представленная на рисунке, показывает на возможность достаточно надежного обнаружения человека-нарушителя на охраняемом объекте. Однако вероятность этого обнаружения зависит от тактико-технических характеристик средств охраны, которые закладываются, исходя из условий их применения, уровня необходимой защиты и, соответственно, возможными затратами на создание ТСО для рассматриваемого конкретного объекта.

Как было сказано ранее, основу комплекса технических средств охраны составляют: средства обнаружения (СО); технические средства наблюдения (ТСН); система сбора, обработки, отображения и документирования информации (ССОИ); средства контроля доступа; вспомогательные средства и устройства. Кроме того, в особо необходимых условиях применяются специальные средства защиты информации, поиска

Рисунок 3.2.1 — Основные типы чувствительных элементов, осуществляющих взаимодействие с внешней средой и нарушителем

техники подслушивания, наблюдения и т. д., а также специальные средства обнаружения и обезвреживания диверсионно-террористических средств.

Предметом рассмотрения являются первые три компонента, т. е. средства обнаружения, технические средства наблюдения и система сбора и обработки информации. Остальные компоненты не могут быть рассмотрены, ибо представляют специальные области знаний, излагаемые в иных учебных программах. Отметим, что важнейшее значение для безопасности объекта имеет применение средств пожарной сигнализации.

В инженерной практике, как правило, выделяются следующие типы средств обнаружения*:

1. *По способу приведения в действие средства обнаружения* подразделяют на автоматические и автоматизированные.

---

* Некоторые названия типов СО могли бы быть объединены, исходя из физических принципов действия их чувствительных элементов или величин измеряемых параметров сигналов.

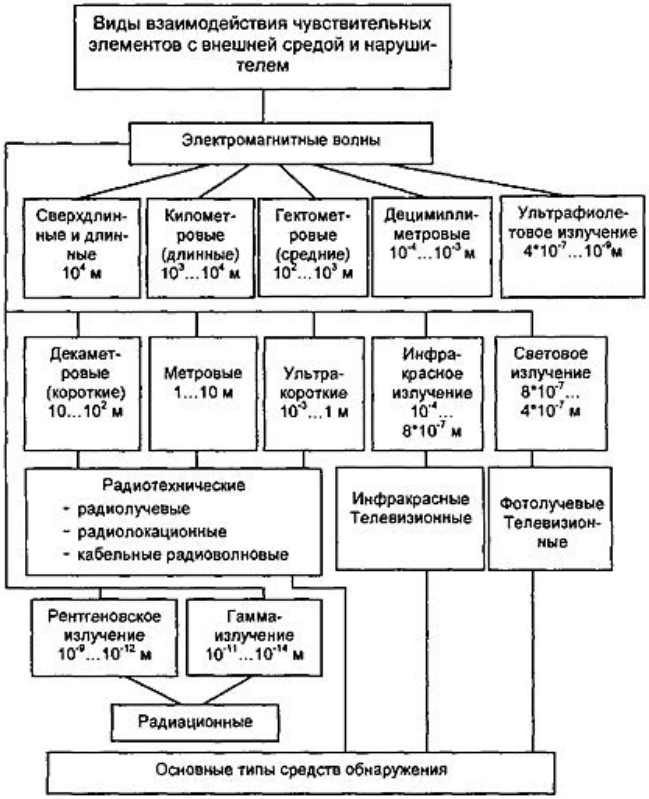


Рисунок 3.2.1 — Основные типы чувствительных элементов, осуществляющих взаимодействие с внешней средой и нарушителем (окончание)

2. *По назначению автоматические средства обнаружения* подразделяют:
- для закрытых помещений;
- для открытых площадок и периметров объектов.

3. *По виду зоны, контролируемой средством обнаружения,* выделяются:
- точечные;
- линейные;
- плоскостные;
- поверхностные;
- объемные.

4. *По принципу действия в системах охранной сигнализации* используются датчики следующих типов:
- пассивные инфракрасные датчики движения;
- активные инфракрасные датчики движения и присутствия;
- фотоэлектрические датчики;
- микроволновые датчики;
- ультразвуковые датчики;

– вибродатчики;
– датчики температуры;
– датчики наличия паров и газов;
– магнитные (герконовые) датчики;
– механические;
– электромагнитные бесконтактные;
– магнитометрические;
– емкостные;
– индуктивные;
– гидроакустические;
– акустические;
– сейсмические;
– оптико-электронные;
– радиоволновые;
– радиолучевые;
– ольфактронные;
– комбинированные.

5. *По количеству зон обнаружения, создаваемых средствами обнаружения,* их подразделяют на однозонные и многозонные.

6. *По дальности действия ультразвуковые, оптико-электронные и радиоволновые средства обнаружения* для закрытых помещений рассматривают:
– малой дальности действия — до 12 м;
– средней дальности действия — свыше 12 до 30 м;
– большой дальности действия — свыше 30 м.

7. *По дальности действия оптико-электронные и радиоволновые средства* обнаружения для открытых площадок и периметров объектов подразделяют:
– малой дальности действия — до 50 м;
– средней дальности действия — свыше 50 до 200 м;
– большой дальности действия — свыше 200 м.

8. *По конструктивному исполнению ультразвуковые, оптико-электронные и радиоволновые средства обнаружения* принято подразделять на:
– однопозиционные — один или более передатчиков и приемник совмещены в одном блоке;
– двухпозиционные — передатчик и приемник выполнены в виде отдельных блоков;
– многопозиционные — более двух блоков.

Каждый из названных классов средств обнаружения представлен на рынке множеством различных датчиков, рассчитанных для применения в конкретных условиях (рис. 3.2.2).

Например, третий класс средств обнаружения может быть представлен в виде рисунка 3.2.2.

Следует отметить, что любой из известных подходов к классификации обладает с точки зрения теории определенными недостатками, например, недостаточной полнотой, в различных классах одних и тех же типов средств обнаружения и т. д. Однако, на практике всегда можно найти подход, удовлетворяющий поставленным задачам выбора или разработки СО для оборудования ими вполне конкретных объектов с вполне конкретными условиями эксплуатации. Например, удобен подход к классификации представленный на рисунке 3.2.3. Его можно назвать подходом, основанным на физических принципах действия чув-

Рисунок 3.2.2 — Классификация СО по виду контролируемой зоны

ствительных элементов средств обнаружения, возможных мест расположения и назначения.

Априори ясно, что выбор конкретного средства обнаружения проистекает из соответствия его тактико-технических характеристик условиям применения. Это означает, что средство обнаружения с данными ТТХ применимо лишь при определенных условиях, т. е. СО должно быть установлено в такой среде, характеристики которой в максимально возможной мере удовлетворяют возможностям выбранного СО, определяемым его ТТХ. Если такой выбор отсутствует, то разрабатывается и производится новое СО, ТТХ которого закладываются заведомо удовлетворяющими условиям эксплуатации, т. е. множеству таких факторов, как:

- климатические;
- биологические;
- геологические;
- механические;
- электромагнитные поля и излучения;
- акустические колебания;
- уровень радиоактивности;
- уровень освещенности и т. д.;
- режимы работы аппаратуры;
- условия электропитания;
- уровень квалификации обслуживающего персонала и т. д.;
- стоимостные и многое другое.

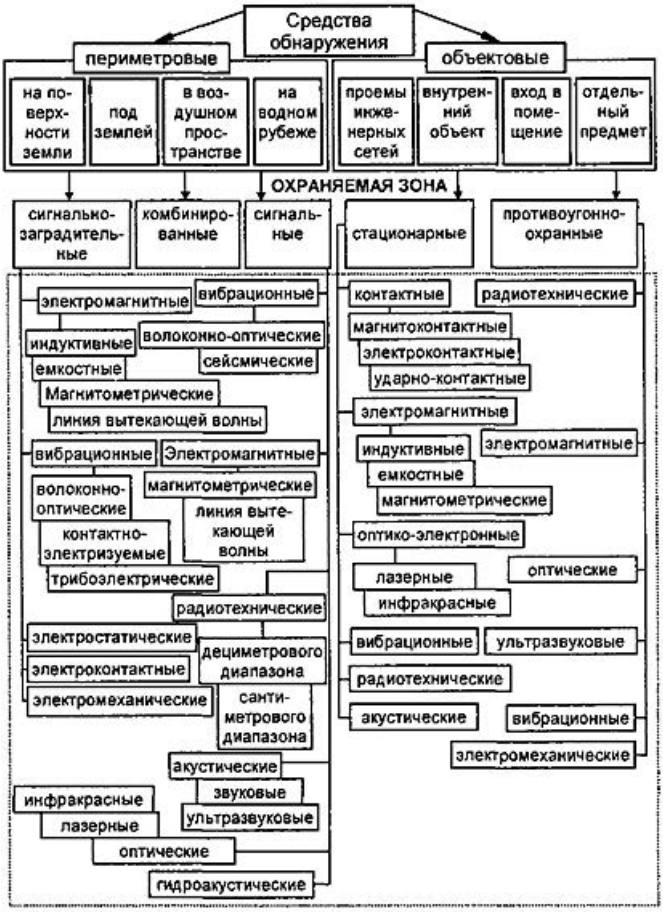


Рисунок 3.2.3 — Пример классификации СО по физическим принципам действия чувствительных элементов и возможным местам расположения

Исходя из тех или иных факторов, обуславливающих применение средств обнаружения, рассматривают следующие основные ТТХ:

– характеристики зоны обнаружения;
– вероятность обнаружения с указанием модели нарушителя;
– наработку на ложное срабатывание;
– чувствительность СО;
– параметры входных и выходных сигналов;
– верхнюю и нижнюю границы скорости перемещения нарушителя;
– время готовности СО после включения напряжения питания;
– время восстановления дежурного режима после окончания сигнала срабатывания;

– требования к параметрам электропитания;
– показатели надежности и ряд других.

Обобщенно в структуре технических средств охраны выделяются три основных компонента:

– средства обнаружения;
– линии передачи сигнала тревоги;
– блоки индикации, регистрации и обработки полученного сигнала.

Кроме того, существуют вспомогательные средства — блоки резервного электропитания, переговорные устройства, прямая телефонная связь с отдаленными объектами охраны и т. д.

Существуют различные подходы и к классификации ТСО, например, исходя из их структуры, назначения, физических принципов действия входящих в него средств обнаружения, типов и схем линий передачи сигнальной информации и по ряду других характеристик. Например, можно предложить классификацию, изображенную на рисунке 3.2.4:

Рисунок 3.2.4 — Пример классификации ТСО

Для охраны внутренних помещений наибольшее распространение получили пассивные ИК-датчики движения и совмещенные датчики типа пассивный + микроволновой.

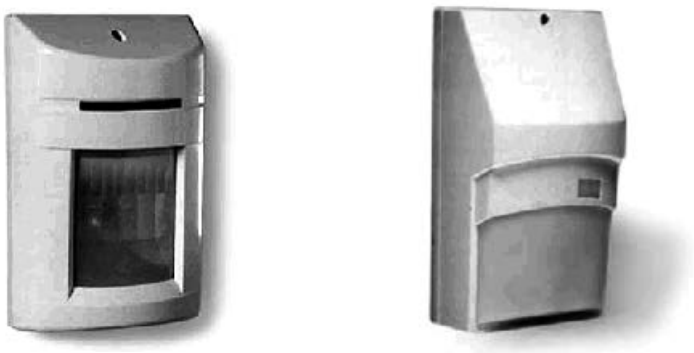
Наибольшей популярностью пользуются датчики:

- серии МН и D&D фирмы CROW;
- серии BRAVO фирмы DSC;
- серии Paradox фирмы PIROTEC;
- серии DXR фирмы CROW;
- серии Force-2 фирмы DSC;
- серии XJ фирмы C&K.

Совмещенные датчики отличает гораздо более высокая надежность и устойчивость к ложным срабатываниям.

Датчики движения (рис. 3.2.5).

Пассивные инфракрасные датчики движения срабатывают при попадании движущегося объекта, излучающего тепло (например, человека), в зону чувствительности датчика. Датчики отличаются, в основном, формой зоны чувствительности и устойчивостью к ложным срабатываниям. Зона чувствительности датчиков для систем охранной сигнализации представляет собой сектор (90–110°). В техническом описании датчиков приводятся диаграммы, которые наглядно демонстрируют зоны чувствительности датчиков. Диаграмма направленности датчика может быть изменена. В соответствии с расположением датчика и особенностями плана помещения изменить диаграмму можно, используя прилагаемые к датчику сменные линзы Френеля или накладки, которые перекрывают часть чувствительного элемента датчика.



а) б)

Рисунок 3.2.5 — Внешний вид датчиков движения:
а) пассивного; б) дуального

Недостаток самых простых и дешевых датчиков в том, что они срабатывают при определенной скорости изменения теплового потока.

Например, при включении/выключении батареи отопления, на сквозняке, из-за нагрева солнцем определенных поверхностей в помещении и т. д. датчик может сработать.

Более совершенные (и более дорогие) датчики не имеют этих недостатков. Их надежность и стойкость к тепловым помехам обеспечивается многоканальными чувствительными головками и сложной обработкой сигнала в самом датчике.

В простых моделях обработка сигналов проводится аналоговыми методами, а в более сложных — цифровыми, например, с помощью встроенного процессора.

К самым простым относятся датчики семейства Bravo-2 фирмы DSC и Paradox Light фирмы PIROTEC. К наиболее сложным — Paradox Vision-510 и UP350 фирмы Alarmcom.

Датчики разбития стекла

Датчики разбития стекла реагируют на звон бьющегося стекла. Наиболее совершенные модели анализируют спектр звуковых шумов в помещении.

Если спектр шума содержит составляющую, совпадающую со спектром повреждаемого стекла, то датчик срабатывает. Один такой датчик может охранять стеклянные окна, витрины и т. п. площадью до 10 м^2.

Двухпороговые датчики регистрируют звук удара по стеклу и звон разбиваемого стекла. Для индикации тревоги такой датчик должен зарегистрировать два соответствующих сигнала с интервалом не более 150 мс.

Чувствительность датчиков разбития стекла регулируется с применением имитатора разбивания стекла, например, марки DG-50 или FG-700.

Фотоэлектрические датчики

Фотоэлектрические датчики излучают и принимают отраженный сигнал инфракрасного излучения с длиной волны порядка 1 мкм. Они используются в составе систем защиты внутреннего и внешнего периметра для бесконтактного блокирования пролетов, дверей, лифтов, проемов, коридоров и т. п. Их отличает высокая устойчивость и надежность работы.

Фотоэлектрические датчики состоят из двух частей — передатчика и приемника (рис. 3.2.6). Они разносятся вдоль линии охраны. Между ними проходит система модулированных инфракрасных лучей.

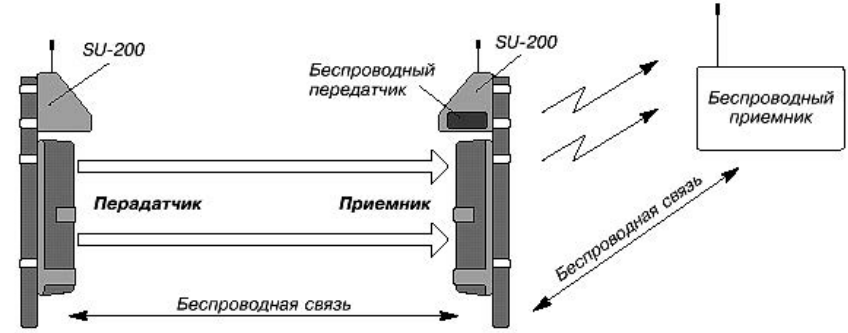


Рисунок 3.2.6 — Фотоэлектрические датчики

Датчики этого типа срабатывают при попытке пересечь систему лучей, отличаются высокой устойчивостью и надежностью работы (рис. 3.2.7).

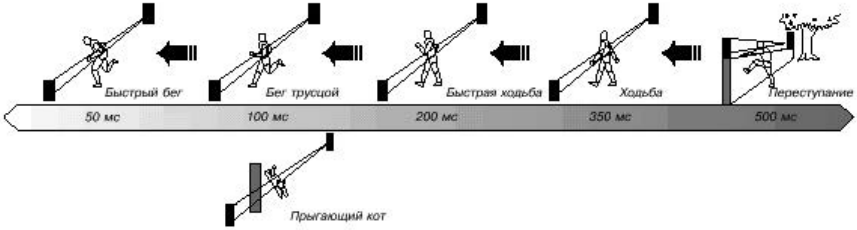


Рисунок 3.2.7 — Варианты срабатывания барьерных датчиков

Наиболее совершенные модели фотоэлектрических датчиков могут работать автономно. Для этого они оснащаются солнечными элементами, которые заряжают аккумуляторные батареи датчиков. Для охраны периметров, при наружной установке (на улице), наибольшее распространение получили активные ИК-датчики фотоэлектрического типа фирмы OPTEX.

Микроволновые датчики

Микроволновые датчики излучают и принимают отраженный сигнал поля сверхвысокой частоты. В плане охраны внутренних помещений, их характеристики аналогичны характеристикам вышеперечисленных устройств, но микроволновые датчики имеют:

– гораздо более высокие цены;
– более низкую устойчивость к ложным срабатываниям;
– высокий уровень вредных излучений.

При охране наружного периметра датчики данной группы проигрывают по своим характеристикам активным ИК-датчикам фотоэлектрического типа.

Ультразвуковые датчики

Ультразвуковые датчики излучают и принимают отраженный сигнал ультразвукового поля. Их отличает:

– малая чувствительность;
– высокий уровень ложных срабатываний;
– зависимость настроек от перепадов температуры, сквозняка, акустических шумов, колебаний влажности.

Поэтому этот тип датчиков нашел применение, в основном, в недорогих системах для защиты малых замкнутых изолированных объемов, например, салона автомобиля.

Вибродатчики реагируют на наличие вибрации и ударов. Работают на основе пьезоэффекта или электромагнитной индукции. Отличаются низкой стоимостью и высоким уровнем ложных срабатываний. Массовое применение находят, в основном, в наиболее дешевых системах автомобильной сигнализации.

Магнитные датчики относятся к самым простым и устанавливаются на окна, двери и люки. Выпускаются двух видов: для наружной и скрытой установки. Обычно размещаются в верхней части двери или окна.

С целью повышения надежности устанавливается по два датчика, соединенных последовательно. При установке на окнах каждая фрамуга окна защищается парой «геркон + магнит».

Магнитные датчики представляют собой пару «геркон плюс магнит» и срабатывают при открытии/закрытии двери или окна. Геркон — это герметически запаянный в стеклянную трубку контакт. Он замыкается или размыкается при поднесении к нему магнита. Обычно магнит крепится к подвижной части двери или окна, а геркон — к неподвижной.

Шлейфы представляют собой ленту из тонкой алюминиевой фольги. Она клеится на стекло, стену, дверь и т. д. При разрушении основания, на которое она наклеена, лента рвется и разрывает цепь протекания электрического тока. Для подключения к цепи охранной сигнализации лента и проводник зажимаются в держателе, который клеится к тому же основанию, что и лента.

Пульт-концентратор принимает сигналы от пультов дистанционного управления и от датчиков охраняемых зон. В зависимости от состояния датчиков, зоны и режима работы, пульт-концентратор включает исполняющие устройства в режимах, заданных пользователем, и запоминает информацию о событиях. Большинство профессиональных пультов-концентраторов имеют встроенный цифровой коммуникационный модуль, предназначенный для приема и передачи кодированных сообщений по телефонной сети в полностью автоматическом режиме.

Коммуникационный модуль позволяет принимать сигнал тревоги по телефону на городском (районном) пульте охраны, оборудованном декодирующей ап-

паратурой, и подавать команды по телефонной линии на пульт-концентратор. Существуют специальные устройства, (например, ESCORT фирмы DSC), позволяющие вести диалог с пультом-концентратором с помощью обычного телефона. Достаточно вызвать телефонный номер, к которому через ESCORT подключен пульт-концентратор, и набрать на телефонном номеронабирателе пароль доступа к системе. После этого пульт-концентратор через голосовой синтезатор устройства ESCORT сообщит текущее состояние и другие запрошенные Вами данные. Весь диалог с системой протекает по принципу: информация от пульта-концентратора — голосовыми сообщениями; Ваши команды — через номеронабиратель.

В зависимости от модели пульт-концентратор позволяет создавать системы охраны как небольших объектов (квартиры, офисы), так и крупных (предприятие, большое здание или комплекс зданий).

Исполняющие устройства

Исполняющие устройства подключаются к центральному пульту с помощью проводной или беспроводной связи. В системах охранной сигнализации могут использоваться следующие исполняющие устройства:

- мощная сирена;
- мигающий свет;
- графические панели с планом помещений;
- система подсветки;
- принтер для регистрации времени, места и характера нарушения и пр.

Наиболее существенным фактором, непосредственно воздействующим на злоумышленника, является звук сирены и мигающий свет.

В качестве сирен используются мощные пьезоэлектрические сирены мощностью до 120 дБ. Более мощные источники звуковых колебаний могут привести к травме слухового аппарата не только нарушителя, но и владельца системы.

Наилучшие образцы сирен для систем охранной сигнализации представляют собой защищенные от механических воздействий устройства с автономным питанием.

Они содержат источники звуковой и световой сигнализации. В случае отключения проводников такие сирены срабатывают, предупреждая о нарушении.

Мигающий свет предназначен для привлечения внимания окружающих при срабатывании сигнализации. Он может включаться как предупредительный сигнал при попытке нарушения подходов к зонам охраны.

Графические панели с планом помещения используются в сложных системах и отображают на плане место нарушения.

§ 3. Системы пожарной сигнализации

Пожарные датчики. По предписаниям СЕАН для каждого учреждения и жилого дома с более чем 10 жилыми единицами положено иметь пожарную сигнализацию. Пожарные датчики, по способу контроля, разделяются на точечные и линейные. Датчики точечного контроля могут быть пороговые, дифференциальные, аналоговые, адресуемые и не адресуемые.

Наиболее простые — пороговые неадресуемые датчики. Срабатывание таких датчиков не позволяет идентифицировать место возгорания и контролировать работоспособность датчика в процессе эксплуатации.

Аналоговые адресные извещатели. Аналоговые адресные дифференциальные пожарные извещатели предназначены для организации охраны средних и крупных объектов с большой концентрацией ценностей в составе автоматических установок пожарной сигнализации с точечным контролем помещений. Все аналоговые адресные извещатели располагаются на двухпроводном кольцевом шлейфе и автоматически адресуются приемно-контрольным устройствам.

Если извещатель кольцевого шлейфа фиксирует сигнал о пожаре, то происходит опознавание группы и конкретного извещателя. При этом сигнал передается в пожарную службу.

Информация о пожаре, содержащаяся в памяти аналогового извещателя, может быть считана приемно-контрольным устройством через интерфейс либо через подключенный к системе МОДЕМ.

В процессе эксплуатации аналоговые дифференциальные извещатели адаптируются к постепенному старению чувствительных элементов, измеряют текущие значения контролируемого параметра и оповещают центральную станцию. По среднесуточному значению контролируемого параметра станцией автоматически корректируется чувствительность аналоговых дифференциальных извещателей и оценивается их работоспособность.

Адрес извещателя устанавливается пластмассовой адресной картой, вставляемой в основание извещателя. Таким образом, основание извещателя становится носителем адреса. Оно не содержит электронных компонентов. Такая конструкция исключает ошибки при техобслуживании, так как адрес устанавливается только один раз в основании и при замене извещателя адрес не изменяется. Адресная карта может быть установлена на заводе с отпечатанным адресом, но можно использовать универсальную карту, адрес которой несложно установить на объекте.

Аналоговые адресные извещатели выпускаются в следующих исполнениях:

- извещатель, регистрирующий изменения температуры;
- оптический дымоуловитель;
- ионизирующий дымоуловитель;
- многофункциональный извещатель с комбинированными чувствительными элементами.

В центральной станции системы противопожарной защиты программируются:

– чувствительность извещателя 0, 1, 2 или 3 (чувствительность — уменьшенная, нормальная, увеличенная или замедленное действие);

– принадлежность извещателя к определенной группе извещателей (с целью индикации состояния извещателей всей группы посредством соответствующих индикаторов на передней панели);

– возможность связи с выходами центральной станции или с выходами адресуемых интерфейсов.

Извещатели серии HP95

Извещатели серии HP95 являются новейшим продуктом английской фирмы APOLLO, поставляемые с марта 1993 года. Они изготовлены с применением технологии поверхностного монтажа электронных компонентов.

Производитель пользовался многолетним опытом, приобретенным при разработке аналоговых адресных извещателей. Восемь лет выпускалась предыдущая серия S90.

Характеристиками новой серии являются:

– совместимость с серией S90 (относительно связи с центральной станцией);
– увеличена надежность передачи данных;
– увеличена разрешающая способность аналого-цифрового преобразователя до 8 разрядов;
– облегчена очистка дымовых коробок благодаря улучшенной конструкции;
– упрощена установка адреса извещателя;
– обеспечена преемственность датчиков;
– у изолятора серии HP95 уменьшено сопротивление (с 50 Ом серии S90 на 0,5 Ом) — это позволяет, соответственно, увеличить сопротивление кабеля шлейфа.

Аналоговый адресный ионизационный дымовой извещатель XP95 Код 55000-500

В извещателе используется источник гамма-излучения америций 241 активностью 33,3 кило-беккереля (0,9 микрокюри).

В двойной ионизационной камере обнаруживается присутствие и измеряется концентрация дымовых частиц. Работа извещателя устойчива и не зависит от параметров окружающей среды.

Аналоговый адресный оптический дымовой извещатель XP95 КОД 55000-600

Дымовой извещатель в оптической измерительной камере по рассеиванию инфракрасных лучей обнаруживает присутствие и измеряет концентрацию дымовых частиц в воздухе. Измеренное аналоговое значение извещатель сообщает центральной станции.

Аналоговый адресный термический извещатель XP95 КОД 55000-401

Термический извещатель измеряет температуру окружающей среды в интервале от 20 до 90 °C и измеренное значение сообщает центральной станции. Существуют два типа термических извещателей — термодифференциальные и термомаксимальные. Первый сам обращается к центральной станции, если разность заданной и измеренной температур превышает установленный предел. Второй — при превышении установленного порога температуры. Центральная станция чаще опрашивает те извещатели, которые обратились самостоятельно, а тревогу поднимает в зависимости от установленных пределов.

Адресный ручной извещатель HOTS КОД 55000-910

В состав ручного извещателя входят электронные схемы, похожие на схемы остальных аналоговых извещателей Аполло. Этот извещатель сообщает центральной станции только два параметра: в нормальном состоянии аналоговое значение 16, а при активированном извещателе аналоговое значение 64. Все остальные значения — ошибки. Активированный ручной извещатель посылает к центральной станции тревожный сигнал прерывания (*interrupt*), независимо от адреса, опрашиваемого в данный момент станцией. Таким образом, центральная станция принимает сигнал от ручного извещателя немедленно.

Изолятор XP95 КОД 55000-700

Изолятор предотвращает выход из строя всего шлейфа в случае короткого замыкания. При этом выпадет только часть шлейфа между двумя изоляторами, которые помещают на каждые 20–30 извещателей или на границе между пожарными секторами. Изолятор вносит в петлю добавочное последовательное сопротивление в 0,5 Ом, которое необходимо учитывать при вычислении падения напряжения в петле.

Изолятор прерывает отрицательный полупериод переменного напряжения, протекающего по петле, а центральная станция — положительный. Таким образом станция защищена от короткого замыкания на корпус объекта.

Световой индикатор (LSI) посредством светоизлучающего диода отображает состояние одного или нескольких извещателей.

Работой индикатора управляет центральная станция через извещатель, к которому подключен индикатор. Несколько извещателей можно подключить параллельно к одному индикатору.

Основание извещателя XP95 КОД 45681-200 одно и то же для всех типов извещателей серии XP95 (кроме ручного, у которого нет основания). Извещатель монтируется в основание, с установленной в него картой адреса. В основание вставлена сменная адресная карта. Носителем адреса является основание, хотя оно не содержит никакой электронной схемы.

Аналоговые адресные пожарные извещатели ESSER серии 9200

Серия 9200 была разработана специально для кольцевых шлейфов сигнализации в приемно-контрольных пожарных системах ЭССЕРТРО-НИК 8008.

Стандартная конструкция цоколя извещателя (модель 781490) может быть расширена в серии 9200 на выход оптокопплера, релейный выход и разделитель групп.

Извещатели серии 9200 соответствуют следующим стандартам и нормативам для приемно-контрольных противопожарных устройств: ДИН/СНЭ 0100, ДИН/СНЭ 0165, ДИН/СНЭ 0833, ДИН 14675, СС 2095, ДИН/ЭН 0108.

На общем кольцевом шлейфе могут подключаться до 127 аналоговых пожарных извещателей серии 9200, входящих в состав 15 отдельных групп.

Особенности извещателей серии 9200:

– встроенная память для хранения информации о сигналах пожара;
– децентрализованный интеллект;
– распознавание первичного и последующих сигналов о пожаре;
– аварийный резерв;
– простой ввод в действие через программную поддержку;
– быстрый, направленный контроль через интерфейс извещателей или по запросу через модем;
– оптическое изображение состояния отдельных чувствительных элементов на дисплее персонального компьютера;
– автоматический контроль чувствительности посредством анализа сигналов динамическими фильтрами;
– бесступенчатая настройка на изменение условий окружающей среды с постоянной скоростью реагирования;
– локализация загрязненного или неисправного извещателя, автоматический надзор;
– возможность поставки в виде многофункционального извещателя с комбинированными чувствительными элементами;
– возможность комбинирования всех извещателей на общем кольцевом шлейфе;
– повышенная эксплуатационная надежность, обусловленная устойчивостью кольцевого шлейфа к коротким замыканиям и прерываниям;
– вид защиты IP40, IP42.

Линейный детектор перегрева и возгорания

Линейный детектор перегрева и возгорания состоит из двух проводов, каждый из которых покрыт терморезистентным материалом. Провода скручиваются в напряженном состоянии. Они спирально обернуты защитной лентой, а снаружи имеют покрытие, соответствующее той среде, где детектор будет использоваться.

Устройство, соединенное с одним концом линейного детектора, создает в цепи постоянный ток. При достижении критической температуры терморезистентный материал размягчается и провода контактируют друг с другом в месте перегрева.

Расстояние до места контакта указывается на центральной панели, в футах или метрах.

Сигнал тревоги подается уже при перегреве, до появления огня или дыма. Детекторы производятся для работы в разных интервалах температур и улавливают разницу между нормальной и повышенной для данного объекта температурой.

Наиболее важно, что кабель линейного детектора может соприкасаться с объектами повышенной пожарной опасности. Термокабель можно проводить над, вокруг или через любую систему, представляющую пожарную опасность. Он будет определять места перегревов гораздо быстрее, чем точечные детекторы, которые устанавливаются на потолке и работают дистанционно.

Детекторы легко сращиваются друг с другом при помощи соединительных устройств. Каждый детектор работает независимо, в своем собственном интервале температур.

Линейный теплодетектор «Protectowrire» имеют следующие особенности:

– обнаруживает перегрев в любой точке и имеет одинаковую чувствительность по всей длине;
– доступен большой диапазон рабочих температур;
– легко сращивается при помощи простых инструментов типа PWS и PWSC;
– простая конструкция позволяет легко обнаруживать неполадки;
– наружная изоляция предохраняет от коррозии, пыли, грязи, повышенной влажности и экстремальных температур.

Пульты-концентраторы

Zarja Electronika

Устройство NJVP-300 предназначено для комбинированной защиты от взлома и пожара. Система пожаротушения управляется автоматически.

Пульт-концентратор NJVP-300 управляет системой технической защиты посредством исполнительных устройств (сирены, световые индикаторы, пожарные люки, электромагнитные клапаны) и обеспечивает передачу сообщений о тревоге на пульт пожарной охраны или полиции.

Максимальная конфигурация NJVP-300 — 6 шлейфов. Для пульта-концентратора NJVP-100 — 1 шлейф.

Каждый модуль NJVP-300 может контролировать состояние одного кольцевого шлейфа. Центральный модуль контролирует состояние всей системы, кольцевых шлейфов на наличие коротких замыканий и обрывов. Устройство имеет модульную конструкцию. Состояние контролируемых секторов отображается посредством светодиодов. К кольцевому шлейфу подключаются до 32 адресуемых устройств. На нем могут находиться интерфейсные устройства для подключения исполнительных устройств, шифраторов, интерфейсов. Они обеспечены источниками автономного питания.

Шифраторы предназначены для включения-выключения групп охранных датчиков с целью доступа в помещения охраняемых зон. Информация о включении/выключении отдельных секторов, взломах и возгораниях протоколируется на принтере.

Контрольная панель ОР-300А позволяет контролировать состояние всей системы и линейных входов на предмет коротких замыканий и обрывов кольцевых шлейфов. Параметры линейных входов устанавливаются программно.

Структурная схема NJVP-300 приведена на рисунке 3.3.1.

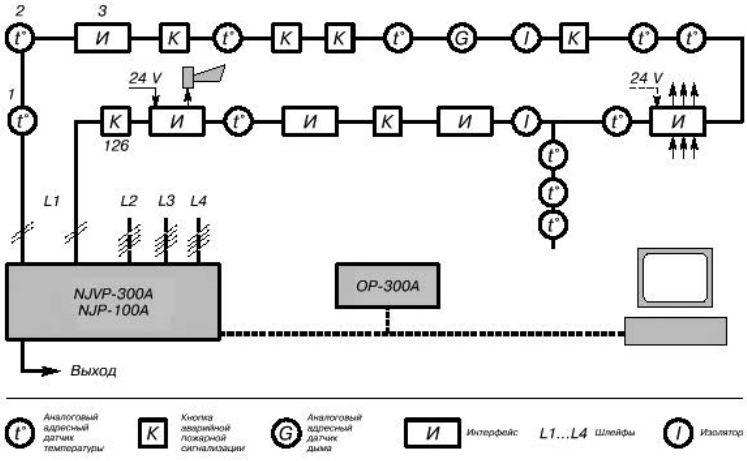


Рисунок 3.3.1 — Структурная схема NJVP-300

Прибор приемно-контрольный пожарный ЭССЕРТРОНИК 3008

Данная система включает 3800 шлейфов сигнализации в 32 подчиненных пожарных контрольных панелях. Обеспечивает возможность подключения до 90 000 пожарных извещателей, относится к числу самых крупных систем в мире.

Пульт-концентратор предназначен для организации охраны средних и крупных объектов.

Одним из преимуществ прибора 3008 является возможность расширения емкости от 8 до 120 шлейфов сигнализации и стольких же исполнительных устройств (на-

пример, реле), что позволяет решать задачи по организации охраны и пожарной сигнализации.

В случае пожара точная информация в виде текста (20 символов) отображается на 4-строчечном жидкокристаллическом дисплее. Наряду со шлейфовыми и диагностическими извещателями, а также описанием места событий, тушение пожара может облегчить и другая информация, специфическая для пользователя.

ЭССЕРТРОНИК 3008 может входить в иерархические системы пожарной сигнализации в качестве основной пожарной контрольной панели (ПКП), в сочетании с подчиненными ПКП такого же типа или типа ЭССЕРТРОНИК 3007. Прибор ЭССЕРТРОНИК 3008 предназначен для охраны больших территорий.

Базовая конструкция рассчитана на контроль 16 свободно программируемых шлейфов сигнализации с адресными пожарными и диагностическими извещателями. Прибор может расширяться с 8 до 120 шлейфов.

Программирование работы шлейфов:

– шлейф пожарной сигнализации формирует сигнал «пожар» при срабатывании извещателей в 2 шлейфах либо при срабатывании 2 извещателей в одном шлейфе;

– промежуточное запоминание тревожных сообщений;

– интерфейсы RS-232 и телеметрический сигнал по линии 20 мА.

ЭССЕРТРОНИК 3008 обеспечивает:

– установку интегрированного печатающего устройства для распечатки текста;

– возможность подключения печатающего устройства с выдачей даты, времени, а также дополнительного текста;

– возможность подключения акустических и оптических сигнальных устройств;

– возможность подключения через интерфейс одного или нескольких параллельных табло индикации;

– возможность подключения компьютера;

– возможность подключения нескольких панелей управления и табло индикации;

– прибор подготовлен для передачи сообщений через системы TEMEX и ISDN;

– передача сообщений на большие расстояния с подключением модемов (VI28);

– возможность подключения 2 главных пожарных извещателей;

– может использоваться в качестве центрального и подчиненного устройства;

– обеспечивает подключение до 32 подчиненных устройств ЭССЕРТРОНИК 3008.

Контрольные панели FS2000 фирмы «Protectowire»

«Protectowire» является лидером в производстве высококачественного противопожарного оборудования и создает такое оборудование, которое не только соответствует всем требованиям заказчика, но и опережает их.

Компания «Protectowire» была основана 50 лет назад. Она начала свою деятельность с создания простейших линейных систем обнаружения перегревов и возгораний.

Сегодня компания производит противопожарную систему «Fire System 2000» с цифровой индикацией точек сигнала тревоги.

Среди поставляемых могут быть выбраны панели, контролирующие до 1067 м термокабеля «Protectowire», до 25 детекторов дыма или панели для подключения неограниченного числа контактных устройств.

«Protectowire» предлагает различные детекторы перегрева и возгорания, а также дополнительное оборудование:

– ультрафиолетовый детектор возгорания;
– пульты ручного управления;
– ионизирующие и фотоэлектрические детекторы дыма;
– устройства световой и звуковой сигнализации.

Панель FS2000 осуществляет полный контроль за состоянием подключенных датчиков и шлейфов. Основная система состоит из двух зон.

Панель обеспечивает независимое тестирование, отключение и переключение каждой зоны, полное управление системами пожаротушения, обнаружение повреждений наружного покрытия и системы заземления.

Управление пожаротушением осуществляется по сигналам охранных шлейфов. Для контроля аварийного затопления на отдельном шлейфе монтируются напольные датчики. Цифровые указатели точек тревоги указывают места обнаружения повышенной температуры и расстояния до них в футах или метрах от начала контролируемого участка цепи.

Сканер зон тревоги может быть установлен на контрольных панелях серий ACR-1600 и FS2000. Он обслуживает 8 или 16 зон, постоянно сканируя их до получения сигнала тревоги. Если такой сигнал будет получен, сканирование прекратится и номер угрожаемой зоны появится на цифровом табло.

Системы подачи предупреждающих сигналов «Protectowire» (рис. 3.3.2) соответствуют требованиям стандартов для защитных сигнальных систем — No. 72 NEPA:

– локальные сигнальные системы;
– вспомогательные сигнальные системы;
– перемещаемые сигнальные системы.

Система «Protectowire» точно указывает место перегрева или возгорания в любой части кабельного желоба.

Теплодетектор может крепиться к жгуту кабеля и проходить по кабельным желобам.

«Protectowire» легко монтируется в оборудовании, и может прокладываться по кабельным желобам и соприкасаться с токоведущими частями, наиболее подверженными перегреву и возгоранию. «Protectowire» может монтироваться везде, где окружающие температуры не превышают собственную термочувствительность.

Система линейного детектирования «Protectowire» типа EPC может работать в агрессивной среде.

На транспортерах пожароопасными могут быть как транспортируемые материалы, так и сами транспортерные ленты. При возникновении пожара огонь быстро распространяется по всей длине транспортера и тушить его очень трудно. Линейные теплодетекторы «Protectowire» устанавливаются над транспортером или на каждой стороне ремня.

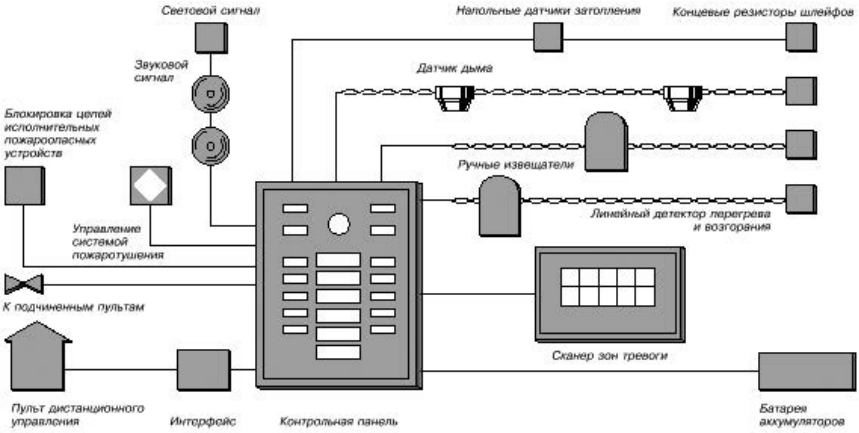


Рисунок 3.3.2 — Противопожарная система «PROTECTOWIRE»

Линейные детекторы «Protectowire» могут быть снабжены электрическими цепями с повышенной защитой, необходимой дня работы на особо пожароопасных участках (классы защиты I, II, III, группы защиты A, B, C, D, E, F, и G).

§ 4. Технические средства и системы защиты внешнего периметра объекта

Тактика оснащения объектов периметральными системами охранной сигнализации должна тесно увязываться с оснащением объекта ограждением, которое призвано задержать проникновение на объект нарушителя на время, необходимое для реагирования лиц, осуществляющих охрану объекта с помощью периметральной системы сигнализации.

Выбор конкретных типов периметральных систем охранной сигнализации производится в зависимости от:

- наличия и вида ограждения (кирпичный забор, сетка рабица и т. п.);
- наличия полосы отчуждения и ее ширины;
- протяженности периметра;
- рельефа местности.

Для защиты периметров объектов рекомендуется использовать следующие виды периметральных систем охранной сигнализации, выполненные на основе:

1. Радиолучевых извещателей, представляющих собой двухблочные технические средства с разнесенными друг относительно друга передатчиком и приемником СВЧ-излучения.
2. Радиоволновых извещателей, представляющих собой специальную систему параллельных проводов, по которым осуществляется приемопередача излучения в определенном диапазоне волн.
3. Радиоволновых доплеровских извещателей.
4. Вибрационных извещателей.
5. Вибросейсмических извещателей.

6. Активных оптико-электронных инфракрасных извещателей.
7. Емкостных извещателей.
8. Проводно-обрывных извещателей.
9. Пассивных оптико-электронных инфракрасных извещателей.
10. Индуктивных извещателей, представляющих собой систему натянутых между опорами ограждения проводов, образующих индуктивную петлю.

В зависимости от принципа действия периметральные системы охранной сигнализации могут блокировать:

– только периметры, имеющие заграждение (заборы): проводно-обрывные, емкостные, индуктивные, вибрационные;

– только периметры, не имеющие заграждения (заборов): пассивные и активные инфракрасные, вибросейсмические, радиолучевые;

– периметры, имеющие и не имеющие заграждения (заборов): проводно-обрывные, радиоволновые, магнитометрические, линии вытекающей волны.

Периметральные системы охранной сигнализации, блокирующие периметры без ограждения целесообразно использовать для охраны особо важных объектов путем установки их перед основным ограждением для упреждения возможного проникновения на охраняемый объект (территорию). Наиболее эффективным из периметральных систем является применение магнитометрической системы, которая может применяться в условиях лесистой местности за счет того, что не реагирует на перемещение животных или людей, не имеющих металлических предметов (холодного или огнестрельного оружия, металлизированных элементов одежды).

Проводно-обрывные системы охраны имеют слабую защищенность от саботажа и, как правило, являются системами одноразового действия, поэтому их целесообразно применять только в комплексе с другими периметральными системами охранной сигнализации.

При оснащении объектов, имеющих ограждения (заборы), в качестве периметральных систем охранной сигнализации рекомендуется использовать в основном емкостные, радиолучевые, радиоволновые, вибрационные, вибросейсмические и пассивные или активные оптико-электронные инфракрасные извещатели.

На выбор типа периметральной сигнализации в первую очередь влияет ее устойчивость к воздействию внешних климатических факторов, которые могут присутствовать на охраняемом объекте. Например, в условиях Беларуси применение активных инфракрасных извещателей связано со многими трудностями, поскольку снежные заносы, растительность, туман вызывают или ложные срабатывания, или отказ системы. Дальность действия пассивных оптикоэлектронных инфракрасных извещателей в условиях тумана или сильного снегопада уменьшается на 25–30 %. Поэтому на местности, где возможно появление туманов, расстояние между извещателями необходимо уменьшать, а в местах поворота периметра либо направлять извещатели встречно друг на друга, либо устанавливать сплошные щиты из досок, изготавливать другие преграды, чтобы компенсировать излишнюю дальность действия извещателей в ясную погоду.

Для дополнительного, визуального контроля, с целью повышения надежности и оперативности службы охраны по выявлению места и характера нарушения, целесообразно применять системы видеонаблюдения. При этом периметр должен оборудоваться охранным освещением с дистанционным управлением из помещения охраны и с автоматическим включением при регистрации тревожных сигналов.

С целью оперативного оповещения о нарушении на участках периметра и отдачи распоряжений по его пресечению рекомендуется предусматривать громкоговорящую и телефонную связь из расчета одна точка на каждом блок-участке.

На контрольно-пропускных пунктах (далее — КПП) объектов, оборудуемых по периметру, необходима установка светоплана периметра с автоматическим высвечиванием участка, на котором произошло нарушение.

Потенциальная восприимчивость основных видов периметральных систем сигнализации к некоторым видам внешних факторов показана в таблице 3.4.1.

Строительные конструкции считаются полностью заблокированы средствами охранной сигнализации, если произведена следующая блокировка:

Окна (витрины) заблокированы:

– на открытие;
– на разрушение (разбитие, выдавливание, вырезание, терморазрушение);
– на выем.

Окна блокируются на открытие с помощью магнитоконтактных извещателей.

Оконные стекла блокируются на разрушение:

– фольгой или проводом ПЭЛ (кроме стеклопакетов с вакуумным межстекольным пространством);
– пассивными звуковыми извещателями для блокировки остекленных конструкций;
– вибрационными извещателями;
– вибрационными извещателями с выносными чувствительными элементами (поверхностными пьезоэлектрическими).

Оконные стекла блокируются на выем с помощью магнитоконтактных извещателей только в тех случаях, когда имеется возможность их выема (выставления) снаружи из обвязки, например, путем отсоединения деревянного или металлического штапика, разбора (развинчивания элементов крепления) рамы, фрамуги.

Использование для блокировки стекол фольги, провода ПЭЛ, пассивных оптико-электронных инфракрасных и вибрационных извещателей не исключает необходимость блокировки оконных стекол на выем.

Двери, ворота, люки заблокированы:

– на открытие,
– на пролом.

Двери, ворота, люки блокируются на открытие магнитоконтактными извещателями. В обоснованных случаях двери, ворога, люки могут блокироваться активными оптико-электронными инфракрасными, инфразвуковыми (давления), ультразвуковыми или радиоволновыми извещателями.

ПКП, подключенные к системе передачи извещений (СПИ), должны эксплуатироваться в режиме «без права отключения», то есть программироваться таким образом, чтобы могли сдаваться под охрану только при исправности всех задействованных шлейфов сигнализации.

Радиоволновые извещатели

Радиоволновые приборы охраны, являясь активными, создают в охраняемом пространстве электромагнитное поле сверхвысоких частот (СВЧ) в диапазоне 3 см с длиной волны 2,8–2,86 см на частотах 10,5–10,7 Гц.

Электромагнитные волны сантиметрового диапазона имеют особенности распространения, влияющие на формирование поля в объеме охраняемого помещения. Прежде всего, необходимо знать, что радиоволны этого диапазона в свободном пространстве распространяются прямолинейно. Предметы, диэлектрическая

Таблица 3.4.1 — Потенциальная восприимчивость основных видов периметральных систем сигнализации к некоторым видам внешних факторов

Внешний фактор	Принцип действия периметральных систем сигнализации				
	Радио-лучевые	Радио-волновые	Вибрацион-ные	Вибросей-смические	Инфра-красн. активные
Температура среды	слабое влияние	слабое влияние	значитель-ное влияние	значитель-ное влияние	значитель-ное влияние
Ветер	слабое влияние	значитель-ное влияние	–	–	–
Дождь	–	слабое влияние	–	–	–
Гроза	слабое влияние	слабое влияние	–	–	–
Град	–	–	–	–	–
Высота снежно-го покрова	значитель-ное влияние	значитель-ное влияние	–	значитель-ное влияние	значитель-ное влияние
Обледенение	значитель-ное влияние	слабое влияние	–	–	–
Туман	–	–	–	–	значитель-ное влияние
Пыль динамическая	–	–	–	–	слабое влияние
Прямой солнечный свет	–	–	–	–	слабое влияние
Переменная облачность	–	–	–	–	–
Неровность грунта	значитель-ное влияние	слабое влияние	–	–	–
Вид грунта	значитель-ное влияние	значитель-ное влияние	–	–	–
Высота травы	значитель-ное влияние	слабое влияние	слабое влияние	–	–

Окончание таблицы 3.4.1

Внешний фактор	Принцип действия периметральных систем сигнализации				
	Радио-лучевые	Радио-волновые	Вибрацион-ные	Вибросей-смические	Инфра-красн. активные
Промышленные помехи	значитель-ное влияние	значитель-ное влияние	слабое влияние	–	слабое влияние
Связные радиостанции	–	значитель-ное влияние	–	–	–
Движение транспорта	–	-	значитель-ное влияние	значитель-ное влияние	–
Промышленная вибрация	значитель-ное влияние	значитель-ное влияние	значитель-ное влия-ние	слабое влияние	значитель-ное влияние
Крупные животные	–	–	–	–	слабое влияние
Мелкие животные	слабое влияние	слабое влияние	–	–	значитель-ное влияние
Птицы	–	–	–	–	–

проницаемость которых отличается от воздуха, являются для сантиметровых волн препятствиями, которые могут быть либо полностью непрозрачными, либо полупрозрачными. В любом случае, наличие таких препятствий приводит к искажению электромагнитной волны, изменению интенсивности поля и направления его распространения.

Основным преимуществом сантиметровых волн, по сравнению со световыми и акустическими, является их практически полная нечувствительность к изменениям и неоднородностям воздушной среды распространения, что существенно повышает помехозащищенность приборов этого диапазона к изменениям ее прозрачности, влажности и насыщенности парами, температуры, подвижности и турбулентности, акустическим колебаниям. В то же время, такие же особенности не позволяют использовать радиоволновые извещатели в качестве пожарных.

Характер воздействия различных препятствий на электромагнитную волну сантиметрового диапазона различен и зависит от материала и размера препятствия, формы и качества его поверхности. По степени воздействия препятствия можно разделить на отражающие, поглощающие и ослабляющие.

Препятствие считается прозрачным, если мощность волны, прошедшей через него, приблизительно равна мощности падающей волны. Примером такого препятствия являются неоднородности воздушной среды распространения. Непрозрачное препятствие может быть отражающим. Примером являются предметы, имею-

щие сплошные металлические поверхности. Непрозрачное препятствие может быть и поглощающим, когда его поверхность проницаема, но в толще материала сантиметровая волна затухает.

Примером могут служить такие предметы, как губчатая резина, ткани, вата, древесно-стружечные материалы большой толщины или заполненные специальными поглотителями.

Препятствия промежуточного типа (ослабляющие) являются полупрозрачными. К ним относятся тонкостенные пластмассовые, деревянные и другие предметы, а также металлические предметы со сквозными щелями и металлические сетки с размером ячеек, сравнимым или бóльшим длины волны. В таблицах 3.4.2 и 3.4.3 приводятся сведения об ослаблении мощности волны трехсантиметрового диапазона в строительных конструкциях и материалах при различных углах ее падения.

В зависимости от формы и качества поверхности препятствий отраженная волна может формироваться по законам зеркального отражения, либо рассеиваться (табл. 3.4.2). Зеркальное отражение происходит в том случае, если передняя граница препятствия является плоской, или ее неровности и шероховатости имеют размеры значительно меньше длины волны. Если же поверхность сложной формы или ее дефекты сравнимы с длиной волны, то отраженная волна рассеивается.

Таблица 3.4.2 — Ослабление мощности СВЧ волны в конструкциях и материалах при перпендикулярном ее падении

Конструкция, материал	Толщина, см	Ослабление, раз
Кирпичная стена	70	120
Железобетонная стена	40	1000
Шлакобетонная стена	46	110
Оштукатуренная стеновая панель	15	16
Слой штукатурки	1,8	6
Межэтажные перекрытия	30	160
Окно с двойной рамой	0,3	1,7
Фанера	–	4–5
Стальная сетка с ячейкой, мм:	0,4	1,2
2,5 × 2,3	–	300
5 × 5,7	–	9,5
8 × 8,7	–	2–3

Необходимо иметь в виду также, что отраженная от препятствия волна взаимодействует с падающей волной, образуя в зоне блокировки так называемую интерференционную картину поля с характерным чередованием максимумов и минимумов мощности (табл. 3.4.3). Наличие минимумов мощности поля, а также зон тени приводит к образованию «мертвых» зон обнаружения нарушителя. Вместе с тем, зоны отражения могут накладываться на зоны тени, создавая возможность для ликвидации таких «мертвых» зон.

Таблица 3.4.3 — Ослабление мощности СВЧ волны в тонких строительных материалах в зависимости от угла ее падения

Материал	Ослабление, раз			
	90°	60°	30°	10°
Щит деревянный, толщина 2 см	2,0	2,5	3	10
Щит ДСП, толщина 1,7 см	1,6	1,6	2	3
Стекло оконное, толщина 0,3 см	2,0	2,5	5	25

Таким образом, изменяя расположение различных предметов внутри охраняемого помещения, можно управлять картиной электромагнитного поля в зоне чувствительности радиоволновых извещателей.

Знание степени ослабления мощности поля в различных строительных конструкциях необходимо учитывать и для оценки влияния внешних помех от источников, работающих на частотах, близких к радиоволновым извещателям (радиорелейных линий, систем управления движением воздушного транспорта, измерителей скорости автотранспорта и т. д.).

Радиоволновые извещатели являются, по существу, миниатюрными радиолокаторами, осуществляющими на основе принципа Доплера селекцию движущихся объектов на фоне отраженного от неподвижных предметов сигнала. Так же, как и в ультразвуковых извещателях, при появлении в области излучения СВЧ передатчика движущегося предмета, частота отраженного от этого предмета сигнала изменяется на величину доплеровского сдвига. Зоной обнаружения извещателя называется часть свободного пространства, движение внутри которого «среднего человека» в течение определенного времени с радиальной скоростью реального перемещения нарушителя, вызывает выдачу извещателем сигнала тревоги. Под «средним человеком» понимается человек ростом около 170 см, весом около 70 кг, движущийся в полный рост. Как радиолокационный объект обнаружения такой человек характеризуется средней эффективной отражающей поверхностью с площадью около 1 м^2. Эта величина принимается в качестве меры для определения параметров зоны чувствительности: максимальной дальности обнаружения и формы зоны обнаружения, характеризующейся значениями ширины в горизонтальной плоскости и высоты — в вертикальной, а также отношений этих величин к максимальной дальности обнаружения. Поскольку формирование зоны обнаружения в описываемых радиоволновых извещателях осуществляется простейшими антенными системами в виде рупора или открытого конца волновода, зона обнаружения имеет каплевидную форму с различной степенью вытянутости, в зависимости от отношений ее размеров. С изменением дальности обнаружения форма зоны чувствительности не изменяется, соотношения ее линейных размеров остаются постоянными, а меняются только их величины.

Необходимо помнить также о том, что описанная форма зоны обнаружения соответствует только открытому (свободному) пространству и является идеальной. В реальных помещениях объектов имеется большое количество различных предметов, являющихся препятствием для распространения трехсантиметровых волн. Стены, пол и потолок помещений также искажают форму зоны обнаружения и формируют «мертвые зоны». Реальные размеры зоны обнаружения и ее форма в кон-

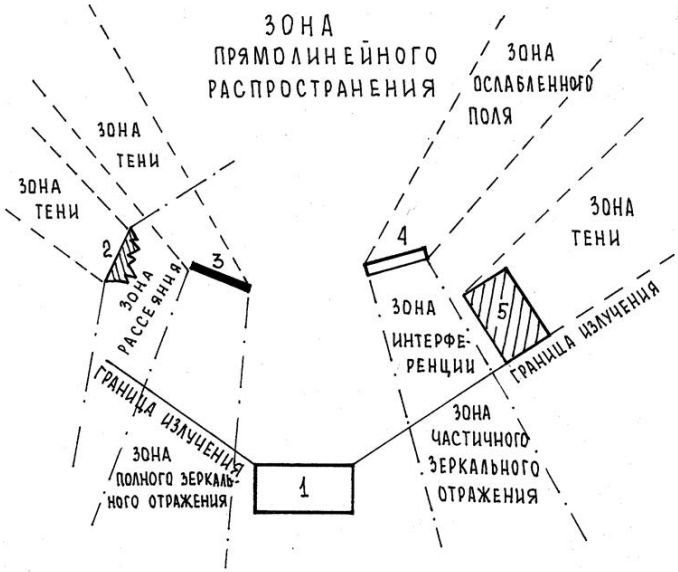


Рисунок 3.4.1 — Электромагнитное поле в зоне чувствительности радиоволнового извещателя:
1 — источник СВЧ излучения; 2 — рассеивающее отражающее препятствие; 3 — плоское отражающее препятствие; 4 — полупрозрачное препятствие; 5 — непрозрачное поглощающее препятствие

кретном помещении могут быть определены только экспериментально в процессе установки и настройки. Форма реальной зоны обнаружения может соответствовать идеальной лишь в пустом помещении с границами из поглощающих материалов или в помещении, размеры которого и расстояния до препятствий превышают размеры зоны чувствительности (рис. 3.4.1).

§ 5. Прикладные проблемы построения систем обеспечения безопасности объектов

Изложенный выше материал преследовал цели формирования у студентов и слушателей:

– общих представлений об охране и защите объектов;

– понимания необходимости системного подхода к решению проблем защиты и охраны;

– знаний и понимания основ систематизации и классификации объектов охраны, моделей нарушителей, технических средств охраны, угроз информационной безопасности, т. е. всего того, что нужно знать и понимать до того как приступать к созданию систем защиты и охраны объектов.

В основе системы защиты объекта лежит принцип создания последовательных рубежей, в которых угрозы должны быть своевременно обнаружены, а их распро-

странению должны препятствовать надежные преграды. Такие рубежи должны располагаться последовательно — от забора вокруг территории объекта до главного, особо важного помещения, такого как хранилище ценностей и информации, взрывоопасных материалов, оружия и т. д.

Чем сложнее и надежнее защита каждой зоны безопасности, тем больше времени потребуется злоумышленнику на ее преодоление и тем больше вероятность того, что расположенные в зонах средства обнаружения угроз подадут сигнал тревоги, а, следовательно, у сотрудников охраны останется больше времени для определения причин тревоги и организации эффективного отражения и ликвидации угрозы.

Кроме средств обнаружения, отражения и ликвидации в систему охраны и защиты входит и специальная защита. К ней относятся все мероприятия и техника борьбы со съемом информации. Несмотря на то, что составными элементами специальной защиты также являются средства обнаружения, отражения и ликвидации угроз съема информации, эту часть системы защиты необходимо выделить отдельно. Специфика и продолжительность подготовки специалистов по защите от съема информации, конфиденциальность и своеобразие их деятельности требуют выделения ее в отдельное направление, которое целесообразнее всего назвать специальной защитой. Всякая информация о структуре, способах и методах организации специальной защиты должна быть строго засекречена.

Важной составной частью системы защиты является персонал службы охраны или службы безопасности. Основной задачей этой службы является поддержание в постоянной работоспособности всей системы защиты.

Следует подчеркнуть, что явное большинство современных средств охраны и защиты представляют собой устройства, работающие на принципах электротехники, электроники и электросвязи.

Основу системы защиты составляют технические средства обнаружения, отражения и ликвидации. Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз. Заборы и ограждения вокруг территории объекта — это средства отражения несанкционированного проникновения на территорию; усиленные двери, стены и потолки сейфовой комнаты защищают от стихийных бедствий и аварий, а кроме того, в определенной мере служат защитой и от подслушивания и вторжения (рис. 3.5.1).

Функции ликвидации угроз осуществляют, например, система автоматического пожаротушения и тревожная группа службы охраны, которая должна задержать и обезвредить злоумышленника, проникшего на объект.

Если возникает необходимость создать систему защиты и выбрать оптимальные с точки зрения затрат технические средства, то удобнее разделить их на основные и дополнительные средства защиты. К основным следует отнести пожарную и охранную сигнализацию, охранное телевидение, охранное освещение, инженерно-техническую защиту.

В последнее время одним из важных направлений защиты становится проверка поступающей на объект корреспонденции на наличие взрывчатых веществ. Следует также проверять и заезжающие на территорию объекта автомашины персонала и посетителей. В связи с этим рекомендуется данный вид защиты отнести к основным.

Специальные средства защиты предназначены для обеспечения безопасности охраняемого объекта от различных видов несанкционированного съема информации и могут использоваться в следующих направлениях:

– для поиска техники съема информации, устанавливаемой в помещениях, технических средствах и автомашинах;

Рисунок 3.5.1 — Обобщенная схема системы охраны и защиты объекта

– для защиты помещений при ведении переговоров и важных деловых совещаний, технических средств обработки информации, таких как пишущие машинки, копировальные аппараты и компьютеры, а также соответствующих коммуникаций.

Дополнительные средства защиты способствуют более оперативному обнаружению угроз, повышают эффективность их отражения и ликвидации. К дополнительным средствам защиты можно отнести:

– внутреннюю и прямую телефонную связь на объекте;

– прямую телефонную связь с ближайшим отделением полиции;

– радиосвязь между сотрудниками охраны с помощью переносных малогабаритных радиостанций. Такой вид связи может использоваться не только сотрудниками охраны, но и персоналом крупных офисов, магазинов и банков;

– систему оповещения, которая состоит из сети звонков и громкоговорителей, устанавливаемых на всех участках объекта для оповещения условными сигналами и фразами о каких-либо видах угроз. Иногда оповещение дополняется сигнальной радиосвязью, малогабаритные приемники которой имеет весь персонал объекта.

Радиосообщения от центрального поста охраны объекта поступают на эти радиоприемники, которые передают владельцу тональные сигналы или короткие буквенно-цифровые сообщения на небольшое табло радиоприемника.

Основным средством обнаружения являются системы сигнализации, которые должны зафиксировать *приближение* или *начало* самых разнообразных видов угроз — от пожара и аварий до попыток проникновения на объект, в компьютерную сеть или сети связи.

Обязательной является пожарная сигнализация, которая представляет собой более разветвленную, чем другие виды сигнализаций, систему и обычно охватывает почти все помещения здания.

Пожарная и охранная сигнализации по своему построению и применяемой аппаратуре имеют много общего — каналы связи, прием и обработка информации, подача тревожных сигналов и др. По этой причине в современных системах защиты эти типы сигнализационных средств иногда объединяются в единую систему охранно-пожарной (ОП) сигнализации. Важнейшими элементами ОП сигнализации являются датчики; характеристики датчиков определяют основные параметры всей системы сигнализации.

Контроль и управление ОП сигнализацией осуществляются с центрального поста охраны, на котором устанавливается соответствующая стационарная аппаратура. Состав и характеристики этой аппаратуры зависят от важности объекта, сложности и разветвленности системы сигнализации.

В простейшем случае контроль за работой ОП сигнализации состоит из включения и выключения датчиков, фиксации сигналов тревоги. В сложных, разветвленных системах сигнализации контроль и управление обеспечиваются с помощью компьютеров. При этом становится возможным:

– управление и контроль за состоянием как всей системы ОП сигнализации, так и каждого датчика;
– анализ сигналов тревоги от различных датчиков;
– проверка работоспособности всех узлов системы;
– запись сигналов тревоги;
– взаимодействие работы сигнализации с другими техническими средствами защиты.

Критерием эффективности и совершенства аппаратуры ОП сигнализации является сведение к минимуму числа ошибок и ложных срабатываний.

Другим важным элементом ОП сигнализации является тревожное оповещение, которое в зависимости от конкретных условий должно передавать информацию с помощью звуковых, оптических или речевых сигналов. Тревожное оповещение имеет ручное, полуавтоматическое или автоматическое управление.

Следует иметь в виду, что тревожное оповещение о возникновении пожара или других чрезвычайных обстоятельств должно существенно отличаться от оповещения охранной сигнализации. При обнаружении угроз чрезвычайных обстоятельств система оповещения должна обеспечить также управление эвакуацией людей из помещений и зданий.

Во многих случаях тревожное оповещение является управлением для других средств системы защиты. При возникновении пожара и его обнаружении, например, по сигналу тревоги приводятся в действие такие средства ликвидации угроз как автоматическое пожаротушение, система дымоудаления и вентиляции. При обнаружении несанкционированного прохода в особо важные помещения может сработать система автоматической блокировки дверей и т. п.

Каналами связи в системе ОП сигнализации могут быть специально проложенные проводные линии, телефонные линии объекта, телеграфные линии и радиоканалы. Наиболее распространенными каналами связи являются многожильные экранированные кабели, которые для повышения надежности и безопасности работы сигнализации помещают в металлические или пластмассовые трубы, металлорукава.

Энергоснабжение системы охранной сигнализации обязательно резервируется.

Исходя из изложенного, основными направлениями деятельности служб безопасности по обеспечению комплексной безопасности являются:

– инженерная и техническая защита территорий, зданий и помещений;
– организация контроля доступа сотрудников и командированных;
– организация охраны особо важных помещений;
– создание систем охранной сигнализации и телевизионного наблюдения;
– разработка рекомендаций по режиму охраны объектов и выработка предложений по работе службы безопасности;
– защита объектов от угроз утечки информации, создание защищенных зон;
– контроль проноса технических средств в особо важные помещения;
– выявление закладных средств подслушивания и видеонаблюдения в помещениях;
– проверка технических устройств обработки информации на наличие каналов утечки и разработка рекомендаций по их защите;
– организация непрерывного технического контроля опасных сигналов в каналах утечки;
– защита объектов от применения диверсионно-террористических средств;
– обеспечение безопасности автоматизированных систем обработки информации от несанкционированного доступа, несанкционированного копирования, вирусной диверсии и других угроз;
– обеспечение применения специальных технических средств контроля особо важных помещений;
– организация контроля телефонных переговоров с их регистрацией.

Создание надежной системы защиты охраняемого объекта от диверсионно-террористических атак предполагает реализацию определенного типового порядка при проведении специальных работ, как то:

– анализ объекта и условий его расположения;
– рассмотрение возможных угроз воздействия на объект;
– специальный анализ ситуации для строящихся и реконструируемых объектов;
– разработка концепции безопасности от всех видов негативных воздействий;
– выработка предложений по техническому оснащению средствами безопасности на основе разработанной концепции и разработка проекта на оборудование инженерно-техническими и специальными средствами;
– приобретение и монтаж специальных технических средств и комплексов;
– обучение персонала приемам и способам использования специальных технических средств, постоянный контроль за эксплуатацией поставленных средств.

Приведем пример. Для решения задач оборудования периметра какого-либо объекта техническими средствами охранной сигнализации предварительно следует знать ответы на вопросы:

1. Какова протяженность периметра.
2. Вид имеющегося заграждения.

3. Количество имеющихся ворот, калиток, их размеры, материал.

4. Ближайшее расстояние от охраняемого рубежа до помещения охраны, до ближайшего к периметру здания.

5. Наличие закладных.

6. Размер зоны отчуждения внутри периметра, наличие кустов и/или деревьев в зоне отчуждения.

7. Необходимость скрытности средств обнаружения.

8. Требуемая точность обнаружения нарушителя на контуре периметра.

9. Требуемое количество рубежей охраны, режимы охраны: круглосуточный, по мере необходимости, N-часовой.

10. Необходимость блокирования: перелаза через ограждения, разрушения ограждения, подкопа под ограждения*.

Приведенный перечень вопросов — минимально необходимый с позиций предварительного анализа, но далеко не полный с позиций системного подхода.

Объективная необходимость построения высокоэффективных систем безопасности объектов в условиях резкого обострения криминогенной обстановки привела к разработке наукоемких интегрированных систем безопасности (ИСБ). ИСБ по существу нацелена на реализацию идей системной концепции обеспечения комплексной безопасности объекта с параллельным решением задач автоматизации управления широкой гаммой систем жизнеобеспечения объекта, как то: энергоснабжением, вентиляцией, отоплением, водоснабжением, лифтовым оборудованием, кондиционированием и т. д.

Среди функций, обязательных для исполнения в контуре ИСБ, следует считать:

– контроль за большим количеством помещений с созданием нескольких рубежей защиты;

– иерархический доступ сотрудников и посетителей в помещения с четким разграничением полномочий по праву доступа в помещения по времени суток и по дням недели;

– идентификацию и аутентификацию личности человека, пересекающего рубеж контроля;

– предупреждение утечки информации;

– предупреждение попадания на объект запрещенных материалов и оборудования;

– накопление документальных материалов для использования их при рассмотрении и анализе происшествий;

– оперативный инструктаж работников охраны о порядке действий в различных штатных и нештатных ситуациях путем автоматического вывода на экран монитора инструкций в нужный момент;

– обеспечение полной интеграции систем видеонаблюдения, сигнализации, мониторинга доступа, оповещения, связи между персоналом СБ, персоналом службы пожарной безопасности, персоналом служб жизнеобеспечения объекта и т. д.;

– обеспечение взаимодействия постов охраны и органов правопорядка при несении охраны и в случае происшествий;

– слежение за точным исполнением персоналом охраны своих служебных обязанностей.

---

* Здесь рассматривается лишь модель физического проникновения. Если же требуется информационная защита — задача охраны многократно усложняется.

Исходя из изложенного ранее ясно, что составными частями ИСБ должны быть:

– сеть датчиков, обеспечивающих получение максимально полной информации со всего пространства, находящегося в поле зрения службы безопасности, и позволяющая воссоздавать на центральном пульте наблюдения и управления всестороннюю объективную картину состояния помещений, всей территории объекта и работоспособности всей аппаратуры и оборудования, включенного в контур ИСБ;

– исполнительные устройства, способные при необходимости действовать автоматически или по команде оператора;

– пункты контроля и управления системой отображения информации, через которые операторы могут следить за работой всей системы в пределах своих полномочий;

– ССОИ, наглядно представляющая информацию с датчиков и накапливающая ее для последующей обработки;

– коммуникации, по которым осуществляется обмен информацией между элементами системы и операторами.

При этом важно наличие возможности оперативного программирования функций ИСБ. Это позволяет противодействовать эффективно таким ухищрениям злоумышленника как:

– прерывание каналов передачи тревоги;

– нейтрализация части системы людьми, имеющими доступ к ее элементам;

– проникновение с сигналом тревоги и уничтожение затем информации о происшествии;

– использование отклонений от предписанного порядка несения службы персоналом охраны;

– создание нештатных ситуаций в работе системы и ряду других.

Тема 4. ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

§ 1. Назначение и структура систем контроля и управления доступом

В настоящее время широкое применение на предприятиях, где необходимо контролировать и ограничивать доступ людей в различные помещения, нашли автоматизированные *системы контроля и управления доступом (СКУД)*. Эти системы предназначены для обеспечения санкционированного прохода в помещения и охраняемые зоны.

Главным направлением развития СКУД является их интеллектуализация, передача максимально возможного количества функций по сбору, обработке информации и принятию решений аппаратным средствам СКУД и компьютерам. Освобождение человека от рутинного труда особенно важно в процессе обеспечения безопасности объектов, где цена ошибки, а подчас элементарной невнимательности, очень велика. С другой стороны, важно обеспечить работника службы безопасности полной и точной информацией о происходящих на объекте событиях и удобными средствами для безошибочного и своевременного принятия оперативных решений.

Системой управления доступом (СУД) называется совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативный контроль за персоналом и временем его нахождения на территории объекта.

Системы управления доступом прошли длительный эволюционный путь от простейших кодонаборных устройств, управляющих дверным замком, до сложных компьютерных систем, охватывающих комплексы зданий, удаленных друг от друга. С помощью СКУД осуществляется автоматизированный контроль доступа в помещения. Это могут быть небольшие системы на 1–3 двери и системы, контролирующие перемещение до нескольких десятков тысяч человек.

Ограничение доступа должно осуществляться без потерь времени и при этом обеспечивать надежный контроль.

Система управления доступом обычно состоит из серверов СУД — обычных компьютеров, которые управляют подключенными к ним контроллерами СУД.

Системы контроля доступа включают считыватели и контроллеры. Считыватель воспринимает информацию, записанную на карточке. Кроме этого он может выполнять дополнительно следующие функции:

- управлять открытием дверей;
- контролировать время, в течение которого дверь открыта;
- контролировать одну зону сигнализации.

Контроллер (контрольная панель) — это специализированный высоконадежный компьютер. В нем хранится информация о конфигурации, режимах работы системы, список людей, которые имеют право входить в помещения, а также их права доступа в эти помещения (когда и куда именно можно ходить). В крупных системах контроллеров может быть несколько. В простых случаях минимальный вариант контроллера может быть встроен в считыватель.

Следующим важным звеном в СУД являются такие устройства, как *считыватели*, которые можно подключить к панели. Считыватель представляет собой устройство, которое позволяет считывать информацию, записанную на карточке. Эту информацию он передает в панель, которая и принимает решение о допуске человека в помещение. Можно настроить панель так, что она будет запрашивать подтверждение принятого решения у компьютера.

§ 2. Элементы систем контроля и управления доступом

В настоящее время применяются разнообразные считыватели самых разных технологий. Любой считыватель предполагает ответную часть — карту, которая содержит информацию, с помощью которой происходит идентификация человека. Каждой карточке приписан некоторый уровень доступа, в соответствии с которым пользователь имеет право прохода через ту или иную дверь в определенные промежутки времени.

Карта может одновременно использоваться как кредитная карта, пропуск с фотографией (нанести фотографию можно с помощью специального принтера для нанесения изображений на пластиковые карты).

Сейчас применяются следующие типы карт, каждому из которых соответствует определенный тип считывателя, который считывает информацию с карты:

- *бесконтактные радиочастотные (PROXIMITY) карты* — наиболее перспективный в данный момент тип карт. Считыватель генерирует магнитное излучение определенной частоты и при внесении карты в зону действия считывателя это излучение через встроенную в карте антенну запитывает ЧИП карты. Получив необходимую энергию для работы, карта пересылает на считыватель свой идентификационный номер с помощью магнитного импульса определенной формы и частоты;
- *магнитные карты* — наиболее широко распространенный вариант. Существуют карты с низкокоэрцитивной и высококоэрцитивной магнитной полосой и с записью на разные дорожки;
- *карты Виганда* — названные по имени ученого, открывшего сплав, обладающий прямоугольной петлей гистерезиса. Внутри карты размещены отрезки проволоки из этого сплава, которые при перемещении мимо считывающей головки позволяют считать информацию. Эти карты более долговечны, чем магнитные, но и более дорогие. Один из недостатков — то, что код в карту занесен при изготовлении раз и навсегда;
- *штрих-кодовые карты* — на карту наносится штриховой код. Существует более сложный вариант — штрих-код закрывается материалом, прозрачным только в инфракрасном свете, считывание происходит в ИК-области.

Для повышения надежности идентификации кроме считывателей к контроллеру может подключаться клавиатура для набора персонального идентификационного номера (ПИН-кода).

Другой тип устройств, которые можно подключить к контроллеру — это охранные панели. Это также специализированный контроллер, который отслеживает состояние охранных датчиков (датчики на дверях, окнах, объемные датчики и другие). Если состояние какого-либо датчика изменяется, то информация об этом тут же поступает в основной контроллер.

У охранной панели может быть набор реле, с помощью которых она может управлять различными исполнительными устройствами. Обычно это электромеханический замок, турникет, лифт, автоматические ворота и т. д.

Традиционные системы контроля доступа идентифицируют пользователя при помощи ключа, введения карточки или набора кода, чтобы разрешить доступ. Применение контактных систем приводит к потере времени при манипуляциях.

Во многих областях, где не допустимы потери времени на действия сотрудников, связанные с обычными системами, оптимальным решением является *бесконтактная система контроля доступа АВАКСЕСС,* которая работает дистанционно в диапазоне низких частот (50–150 кГц). Она позволяет осуществлять бесконтактную идентификацию карточек и запрограммированных в них кодовых номеров. Позволяет считывать код через такие материалы, как одежда, сумки и стены.

Несмотря на проведение большого количества проверок в целях безопасности, этот процесс происходит для пользователя автоматически и быстро. Для тех, кто имеет право доступа, входная дверь кажется незапертой.

Благодаря применению бесконтактной технологии становятся невозможными манипуляции со считывателями. Разрешение на те или иные действия дается исключительно в подсистемах или в центральном компьютере, которые устанавливаются на защищенном участке.

Даже повреждение считывателя ни при каких обстоятельствах не даст возможности несанкционированного открытия двери.

Считыватели, в первую очередь на внешних входах, должны монтироваться таким образом, чтобы они были закрыты, или устанавливаться на защищенных участках дверей или стен. Благодаря этому уменьшается также риск повреждения, а установленные элементы становятся недосягаемы.

Система АВАКСЕСС позволяет провести большое количество проверок в целях безопасности и в то же время избавить пользователя от процедуры идентификации.

Практически невозможно подделать карточки АВАКСЕСС и их функции. Карточка запатентована во всем мире и используемый в ней микрочип был разработан специально для этого изделия.

Кодирование карточек и систем осуществляется производителем в Швейцарии фирмой «АВАТЕХ АГ». Это, с одной стороны, увеличивает безопасность в отношении структурирования номеров кодов и, с другой стороны, позволяет более гибко формировать и размещать кодовую информацию.

Имеющийся в карточке объем информации 65 бит разбит следующим образом:

- 16 бит для кода страны;
- 16 бит для кода клиента;
- 32 бит для кода пользователя (например, текущие номера для сотрудников);
- 1 бит для признака статуса контроля функции карточек.

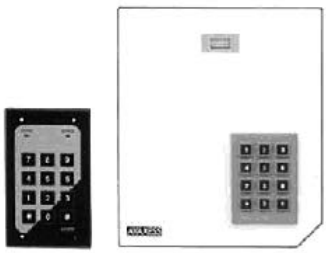
Если карточка теряется, ее сразу же можно аннулировать. Таким образом, исключается опасность несанкционированного доступа при помощи потерянной или украденной карточки.

Считыватели системы монтируют в двери, рамы двери, перегородки/стены и кабины лифта таким образом, чтобы они были полностью скрыты от глаз. В оформлении считывающих элементов учитываются эргономические и эстетические требования. Ядро системы располагается на защищенном участке.

Считыватели в контактных системах часто выходят из строя. Этого не наблюдается при применении считывателей АВАКСЕСС, где нет контакта с руками. Какой-либо сбой устраняется при помощи программ индикации сбоев и диагностики.

Система имеет модульное построение и отдельные элементы можно легко заменить. Система может быть расширена без замены имеющейся аппаратуры. Можно поставить под контроль дополнительные входы и подъезды или ввести дополнительные функции, как, например, учет времени присутствия сотрудников или посетителей.

Контроль доступа с кодом. Для участков, к которым предъявляются повышенные требования к безопасности, бесконтактный считыватель дополнительно оснащается клавишной панелью.



Функция ввода кода может по времени индивидуально включаться или выключаться на каждую дверь. Если используется клавишная панель, то пользователь должен вначале считать карточку. Этот процесс включает кодовую клавиатуру.

Пользователь набирает свой личный код, и при наличии права доступа осуществляется открытие двери. Личный код у каждого сотрудника индивидуален, он сравнивается и сверяется с его карточкой.

Код может набираться сотрудником при первичном пользовании системой и также позже может им самостоятельно меняться. Если это нежелательно, то администратор системы определит кодовые номера для отдельных сотрудников.

Кодовая клавиатура позволяет также вводить код тревоги в случае угрозы данному сотруднику со стороны постороннего лица (тихая тревога).

Управление дверьми

В рамках программы АВАКСЕСС можно производить контроль и управление всеми оснащенными считывателями дверьми, а также дверьми без считывателей.

Контролируется заранее заданное максимально разрешенное время открытия двери. При слишком длительном времени открытия подается сигнал тревоги. Первый сигнал тревоги дается акустически у двери. Это позволяет закрыть дверь без каких-либо дальнейших последствий. Если дверь продолжает оставаться открытой, то дается основной сигнал тревоги с протоколированием в главной системе АВАКСЕСС.

Тревога может передаваться также и в другое место или на другую систему.

При помощи программного обеспечения двери могут отпираться на определенный период времени. Например, дверь может быть открытой, каждый рабочий день с 8.00 до 17.00.

Можно также запрограммировать систему так, чтобы открытие утром (с 8.00) осуществлялось только после считывания первой карточки (например, в 8.14, когда вошел первый человек). Таким образом, открытие двери осуществляется только тогда, когда в соответствующей зоне находится лицо, имеющее право доступа.

Каждая дверь посредством дополнительных интерфейсов может соединяться с охранной и противопожарной системой при двойном контроле доступа.

Управление шлюзом. При двойном контроле доступа ведется протоколирование движений на входе и выходе. При этом используются специальные кабины — шлюзы.

В таблице приведены схемы и краткие характеристики различных вариантов шлюзов.

Фиксация прохождения шлюза производится только тогда, когда проход фактически завершен. Это предотвращает неправильную фиксацию, например, в ситуации, когда карточка считывается, а сотрудник принимает решение не проходить через шлюз. Через шлюз может пройти только один человек. В них устанавливаются два считывателя на входе и выходе. Если человек вошел в шлюз, то он должен вначале выйти, чтобы иметь возможность войти снова.

Право доступа в лифт

Пользование лифтом может осуществляться также при помощи карточки. Определенные этажи могут быть заблокированы, а вход на них может осуществляться только при наличии права доступа. Можно также вызвать лифт на определенные этажи карточкой вместо кнопки вызова и тем самым ограничить пользование лифтом.

Регулирование потока посетителей

Посетители могут получать право доступа в выделенное для них время. Все посещения могут фиксироваться с различными данными по посетителю.

Эта информация хранится в системе и может быть в любой момент запрошена по различным критериям поиска. Можно также распечатать для посетителя пропуск с фамилией, названием фирмы и датой.

Контроль въезда

Если при въезде водители автотранспорта будут держать карточку сбоку у окна автомобиля, идентификация осуществляется автоматически на расстоянии. При наличии права доступа с центрального пульта АВАКСЕСС передается сигнал на открытие ворот или шлагбаума.

Предусмотрены специальные карточки, которые могут крепиться на автомобилях (например, автомобиле директора, фирменных служебных автомобилях и т. д.). Карточки, смонтированные на днище автомобиля, автоматически считываются и проверяются при пересечении заложенной в полотно дороги петли. Это позволяет провести идентификацию без каких либо операций. Скрытая проволочная петля защищена от любого вида повреждений или манипуляций.

Для автомобилей любого типа совместно с системой АВАКСЕСС может использоваться считыватель SmartPass (рис. 4.2.1). SmartPass работает в диапазоне высоких частот (2,4 ГГц) и позволяет идентифицировать движущиеся автомобили. Используя SmartPass, можно реализовать контроль въезда, транспортировку товаров и пр. На считыватель не влияют атмосферные условия и он может идентифицировать карточку на расстоянии до 6 м.

Рисунок 4.2.1 — Идентификация и регистрация транспортных средств антенным считывателем SmartPass

Учет времени

Система контроля доступа АВАКСЕСС позволяет также реализовать скользящий график работы сотрудников. При этом карточка АВАКСЕСС может «отмечаться» на терминале учета времени. В зависимости от требований и объема системы используется один компьютер на две области применения или две отдельных системы.

Имеется полное программное обеспечение для учета рабочего времени сотрудников. Структура этого решения учитывает требования, наиболее часто выдвигаемые заказчиком, экономит расходы и упрощает обращение с системой.

Элементы системы АВАКСЕСС:

1. Карточки АВАКСЕСС. Изготавливаются в виде брелока для ключей или в виде карточки. Карточка может использоваться также в сочетании с пропуском на бумаге для дополнительного визуального контроля. Этот пропуск по индивидуальному желанию может быть оформлен текстом, фотографией, штриховым кодом или магнитной полоской. Карточки программируются в соответствии с требованиями клиентов. По дополнительному требованию, они могут перепрограммироваться, а в случае расширения системы или потери могут быть получены дополнительные карточки. Специальный вариант для автомобилей всех видов используется для контроля въезда и регистрации. Карточка крепится в зависимости от требований на днище или сбоку автомобиля.

Кроме бесконтактных карточек, в системе АВАКСЕСС могут использоваться магнитные карточки, карточки с чипами и ключи с чипами. Эти виды пропусков позволяют осуществлять как функцию считывания, так и записи.

2. Антенные считыватели АВАКСЕСС (рис. 4.2.2):

– Миниатюрный антенный считыватель. Включает в себя передающую и приемную часть для бесконтактной идентификации карточек АВАКСЕСС. Приспособлен для монтажа на стене или в стене. Создает поле опроса радиусом до 90 см и оборудован индикатором состояния. Выпускается в настольном варианте.

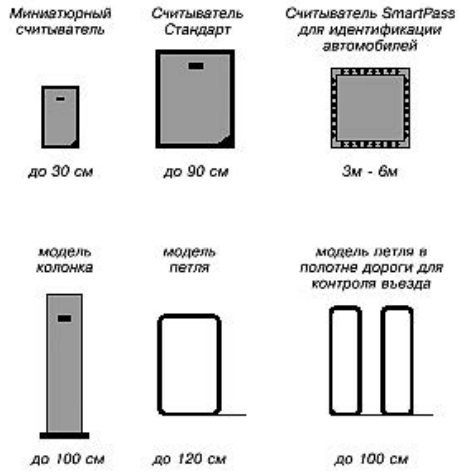


Рисунок 4.2.2 — Антенные считыватели АВАКСЕСС

– Антенный считыватель стандарт. Включает передающую и приемную часть для бесконтактной идентификации карточек АВАКСЕСС. Создает поле опроса радиусом до 90 см. Приспособлен для монтажа на стене или в стене и оборудован индикатором состояния и сигнальной сиреной для двери.

– Антенный считыватель дальнего диапазона в виде петли. Состоит из антенной петли и блока согласования для бесконтактной идентификации карточек АВАКСЕСС. Создает поле опроса радиусом до 120 см. Предназначен для установки в дверях, около дверей или в стенах.

– Автомобильная антенная петля. Используется совместно с блоком согласования для бесконтактной идентификации карточек АВАКСЕСС. Создает поле опроса над проезжей частью радиусом до 100 см. Подходит для идентификации/регистрации автомобилей любого вида.

– Считыватель SmartPass. Предназначен для контроля въезда, а также для идентификации автомобилей при контроле графика их работы. Оборудован встроенной системой считывания на радиочастоте. Состоит из принимающей и передающей части, декодера и сетевого блока. Прочный и устойчивый к атмосферным воздействиям корпус для простой инсталляции в любых условиях. Идентифицирует стоящие и движущиеся автомобили всех видов на расстоянии до 6 м.

– Антенный считыватель дальнего диапазона в виде колонки. Состоит из пластмассовой колонки, устойчивой к атмосферным воздействиям, передающей и приемной части для бесконтактной идентификации карточек АВАКСЕСС. Создает поле опроса радиусом до 100 см. Пригоден для контроля доступа людей и въезда автомашин в зону стоянки, для внутренней и внешней инсталляции. Система АВАКСЕСС может работать совместно с системами безопасности.

К интерфейсу считывателя АВАКСЕСС могут быть подключены все бесконтактные считыватели. Это позволяет реализовывать системы считывания с радиусами действия от 5 см до 1,5 м, которые выбираются в зависимости от потребности.

Технические характеристики системы АВАКСЕСС

Система АВАКСЕСС 100. Система 100 — это автономная электронная система запирания дверей для одного бесконтактного считывателя. Возможно хранение в памяти системы до 899 лиц и/или автомобилей с применением временных критериев доступа. Система отличается простым обслуживанием и высокой степенью надежности. Центральный блок системы 100 со считывателем модели стандарт и миниатюрным считывателем (рис. 4.2.3).

Встроенное табло позволяет производить программирование всех функций и прав доступа. Не требует специального устройства для программирования. Может вести протоколирование всех перемещений на принтере, а также осуществлять контроль дверей с выдачей сигнала тревоги.

Стандартные интерфейсы позволяют стыковать систему с системами телеуправления, оповещения о пожаре и охранными системами.

Мощное программное обеспечение позволяет идентифицировать до 30 000 лиц, подключить до 2048 считывателей и клавишных кодовых панелей. Программное обеспечение используется для учета и поддержки (изменения), а также опроса событий.

Отдельные контроллеры могут быть расширены в 2 этапа до 8 антенных считывателей или клавишных панелей. Контроллеры подключаются к интерфейсу RS485. Система 500 может использоваться и для контроля за аварийными выходами или окнами и позволяет оптимально скомбинировать контроль доступа

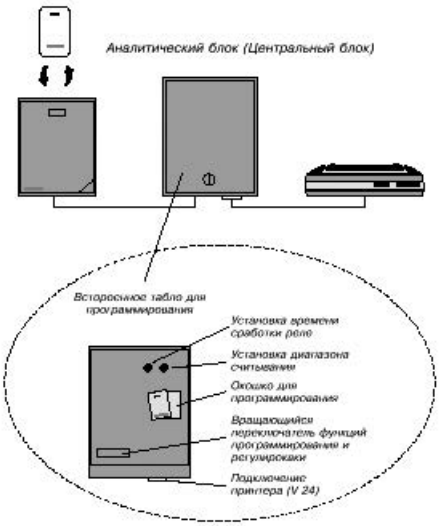


Рисунок 4.2.3 — Центральный блок системы 100

и общий контроль. Предлагаются различные варианты запросов, по которым может быть получена информации о присутствующих или о месте и времени перемещения отдельных лиц.

Система АВАКСЕСС 500

Система 500 предлагает всеобъемлющее решение для контроля доступа и управления дверьми. АВАКСЕСС 500 подходит для средних и больших конфигураций охранных систем и может быть включена в общую концепцию безопасности (рис. 4.2.4).

Программное обеспечение АВАКСЕСС

Программное обеспечение системы 500 работает в среде MS-DOS и Windows. В зависимости от размера системы и требований имеется три различных версии программного обеспечения. Автономность контроллеров ПК позволяет работать в многозадачном режиме. Последняя версия программного обеспечения выполняет следующие функции:

– подключение различных языковых версий;
– банк данных, совместим с D-Base III;
– двойной контроль доступа;
– 64 временных интервала по 10 временных зон на каждый временной интервал;
– календарь отпусков на 3 года;
– автоматическое переключение летнего/зимнего времени;
– системы тревожной сигнализации на дверях с контролем разрешенного времени открытия, взлома двери, разрыва линии, преднамеренного повреждения;
– контроль дверей без считывателей (например, аварийных выходов, окон и пр.);
– многоступенчатую функцию паролей для оператора.

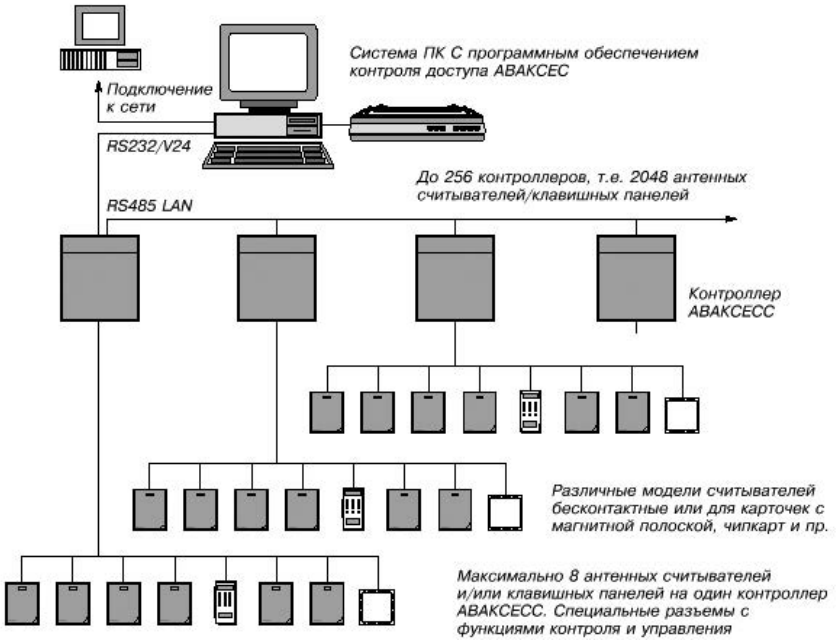


Рисунок 4.2.4 — Структурная схема системы АВАКСЕСС 500

Тема 5. ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОИЗВОДСТВА

Оперативно-розыскной процесс можно определить как применение в определенном порядке компетентными должностными лицами оперативных подразделений органов, осуществляющих оперативно-розыскную деятельность, положений оперативно-розыскного законодательства и детализирующих их норм подзаконных нормативных актов в интересах решения задач оперативно-розыскной деятельности (ОРД) сообразно предусмотренным законом основаниям проведения ОРМ.

Под ним мы понимаем основанную на законе и облеченную в форму правовых отношений деятельность правоохранительных органов, использующих негласные и иные специальные силы и средства, а также участвующих в ней лиц. Причем эта деятельность осуществляется в целях предупреждения совершения преступлений, поиска событий преступлений и розыска лиц, уклоняющихся от правосудия, а также с целью способствования решению задач уголовного судопроизводства и уголовно-исполнительного производства.

Необходимо отметить, что характерная черта оперативно-розыскного процесса в том, что его участниками, действующими под руководством персонала оперативных подразделений, нередко являются частные физические лица:

а) гласно содействующие оперативным аппаратам как их внештатные сотрудники;

б) конфиденциально сотрудничающие с оперативными аппаратами. Эти участники оперативно-розыскного процесса имеют конкретные обязанности и права, которые закреплены на законодательном и ведомственном уровне.

Для оперативно-розыскного процесса свойствен определенный круг субъектов, усилиями которых он осуществляется.

В их числе:

- персонал оперативных подразделений, обладающих полномочиями в полном объеме применять все ОРМ и действовать на всех стадиях производства по отдельным материалам или делам;
- частные физические лица, гласно или конфиденциально содействующие сотрудникам оперативных подразделений;
- сотрудники различных служб, осуществляющие оперативно-розыскную деятельность, действующие, как правило, по заданиям и поручениям сотрудников оперативных подразделений.

Объектом оперативно-розыскного процесса являются сфера и инфраструктура социально-аномальных проявлений, прежде всего противоправных, совершаемых, как правило, профессионально и организованно.

§ 1. Оперативно-розыскное производство как реализация оперативно-технических форм оперативно-розыскной деятельности

Опыт оперативных работников (работников уголовного сыска) передавался через поколения как повторение оправдавших себя на практике навыков, приемов и традиций. Все они основаны на знаниях человеческой натуры, законов преступ-

ного мира, а также на профессиональной интуиции и нестандартных оперативных решениях.

В советский период из-за различных бюрократических преград и ведомственной волокиты многие технические средства не внедрялись в ОРД, что обеспечивало техническое превосходство криминальной среды общества над правоохранительными органами.

Однако накопленный в отдельных оперативных подразделениях опыт использования технических средств долгие годы имел ограниченное распространение. Всесторонний критический анализ использования специальной техники в деятельности правоохранительных органов не производился. Это негативно отражалось на организации и практическом осуществлении оперативной работы и повлекло создание «заинтересованными лицами» целой системы мер по ее компенсации. Так, преступники, задержанные с поличным, нередко использовали сведения, доказывающие «провокационный» характер оперативно-розыскной деятельности. В специальной литературе 1970-х годов приводятся примеры, когда взяточники заблаговременно готовили аргументы для снятия с себя возможного обвинения. Для этого задним числом писались жалобы прокурору о «незаконных» действиях оперативников, «постоянно подслушивающих телефонные переговоры и помечающих купюры, переданные в качестве возврата долга».

И сейчас преступниками заранее учитывается вероятная фиксация их действий при помощи технических средств: отслеживается персональный состав оперативников и участников следственных действий, организуются поиски агентов внедренных в преступную среду. Делается это для того, чтобы поставить под сомнения доводы обвинения. Поэтому постоянно существует необходимость принятия неординарных организационных, тактических и технических решений.

В ныне действующем Федеральном Законе об ОРД предпринята четвертая за российскую историю законодательная попытка регламентировать порядок внедрения в преступную среду штатных сотрудников правоохранительных органов. Первые три оказались неудачными.

Во многих зарубежных странах этому вопросу уделялось самое пристальное внимание. Например, в США только за период с 1924 по 1934 год было принято 14 законов, касающихся оперативно-розыскной деятельности Федерального бюро расследований. Верховный суд США сформулировал принципы, известные под названием «привилегии информаторов», в соответствии с которыми полиции было предоставлено право не раскрывать их личность. Информаторы получили право в исключительных случаях выступать в суде в качестве свидетелей. Правительство при этом гарантировало их защиту и неразглашение личных данных.

Для получения оперативной информации в развитых странах сейчас введен запрет на применение технических средств, психотропных, химических и иных веществ, которые угнетают волю или вредят здоровью человека. Ограничения прав человека и гражданина, допускаемые во время проведения ОРМ, носят временный характер и могут осуществляться лишь с санкции прокурора. Закон запрещает привлекать к выполнению заданий оперативных подразделений священнослужителей, медицинских работников и адвокатов в случаях, когда лицо, от которого они должны получить информацию, является их пациентом, клиентом, прихожанином.

Собрать необходимую информацию о преступлении и преступниках без эффективного использования разнообразных технических средств стало сейчас прак-

тически невозможно. Поэтому Федеральный Закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (Закон об ОРД) предусматривает использование в ходе проведения ОРМ информационных систем, видео- и аудиозаписи, кино- и фотосъемки, а также других технических средств, не наносящих ущерба жизни и здоровью людей, не причиняющих вреда окружающей среде.

Это связано с тем, что техника позволяет изучить не воспринимаемые в обычных условиях события и факты, обобщить имеющуюся информацию, позволяет увеличить ее поток, облегчает мыслительную деятельность человека и оценку достоверности выводов.

Применение техники в ОРД должно связываться, прежде всего, с расширением возможностей чувственного познания.

Органы чувств человека — зрение, слух, обоняние и т. д., сами по себе не являются высокоточными средствами чувственного отображения. В ситуации, связанной с раскрытием преступлений, нельзя, безусловно, опираться на их непогрешимость. Любые показатели органов чувств, необходимо тщательно проверять. Это связано с тем, что многие явления и процессы, происходящие в реальной жизни, человек просто не в состоянии воспринимать. Например, звуковые колебания воспринимаются им только в пределах от 16 Гц до 20 кГц. Иная частота колебаний не вызывает у людей никаких слуховых ощущений.

Зрительное восприятие возникает лишь при воздействии на глаз электромагнитных колебаний с длиной волн от 380 до 760 см. По сравнению с полным диапазоном колебаний, ныне известных науке, участок этот неимоверно мал. То же касается и других органов чувств.

Пороги чувствительности у разных людей далеко неодинаковы. В течение жизни они подвержены различным изменениям у одного и того же человека, находясь в прямой зависимости от состояния физического и психического здоровья, возраста, наличия заболеваний, условий проживания и многого другого. Для того чтобы как можно глубже проникать в сущность любых вещей и явлений, необходимо расширять возможности знания через применение различных технических приспособлений. В настоящее время с применением специальных технических средств правоохранительными органами России раскрывается более 75 % преступлений, совершенных в условиях неочевидности.

Применение техники в ОРД не сводится только к получению разнообразной информации. Техника предназначается еще и для облегчения восприятия сведений конкретным человеком, который, в свою очередь, должен быть способен к их анализу, переработке, сохранению и передаче по назначению.

Даже при наличии достаточного времени для анализа и дальнейшей работы с полученной информацией, оперативный работник в состоянии переработать лишь определенный ее объем. Если же объем полученной оперативной информации превышает «пропускную способность» органа чувств оперативного работника, то она не будет воспринята и переработана. В таких случаях технические средства незаменимы. Они позволяют преобразовывать и регулировать большие информационные потоки, либо хранить нужные сведения в течение времени, необходимого для ее последующего восприятия и переработки.

В оперативной работе проанализировать информацию и сделать соответствующие выводы чаще всего недостаточно. Получаемую информацию нужно уметь запомнить. Именно профессиональная память оперативного работника (оперативника) в конечном итоге формирует возможность сравнения и выбора, определяет интеллектуальную самостоятельность и рабочую инициативу.

Слабая сторона памяти состоит в том, что при воспроизведении ранее полученной информации они невольно привносят субъективные элементы, так или иначе искажающие ее. Иногда искажения приводят к возникновению различных критических ситуаций или к наступлению необратимых процессов. Если же объект фиксируется при помощи технических средств, то сравнивая зафиксированные сведения с теми, которые остались в памяти оперативного работника, можно установить и скорректировать практически все привнесенные извне субъективные элементы.

Технические средства играют важную роль в запоминании, сохранении и воспроизведении информации, полученной оперативным путем, позволяя на основании собранных данных быстрее прийти к выводам о существовании различных закономерностей и связей.

§ 2. Технические средства обеспечения оперативной работы

Сегодня популярны дискуссии об «эффективности» использования таких негласных средств, как прослушивание телефонных и других переговоров, негласное проникновение в помещение, визуальное наблюдение с использованием фото-, кино- и видеосъемки, перлюстрация почтово-телеграфных отправлений и пр. Нередко речь идет о нарушении конституционных гарантий неприкосновенности жилища, личной жизни граждан, тайны телефонных, телеграфных и письменных сообщений. Однако при наличии определенных оснований действующим законодательством предусматривается не только осуществление перечисленных ОРМ, но также их обеспечение средствами специальной техники.

Номенклатура современных технических средств и аксессуаров включает более 20 групп, в которые входят:

- средства оперативной связи;
- системы поиска и слежения за подвижными объектами;
- средства негласного доступа в помещения;
- средства маркирования объектов;
- программные средства;
- штурмовое оборудование;
- системы подавления радиосредств, средства радиомониторинга, системы пеленгации;
- взрывозащитные и пулестойкие конструкции и материалы;
- коммутаторы, телефонные станции с автоматическим определением номера;
- средства обнаружения радиоактивных материалов, взрывчатых и химических веществ;
- рентгеноскопическое оборудование;
- обнаружители оружия;
- роботизированные комплексы;
- средства жизнеобеспечения в экстремальных условиях и многое другое.

В эти группы входят как общедоступные (приспособленные), так и специально разработанные технические средства, применяемые исключительно для решения задач, возникающих в процессе ОРД. Так, например, использование связи или приборов наблюдения на расстоянии, как правило, носит вспомогательный характер. С помощью радиостанций обеспечивается четкость взаимодействия между оперативными сотрудниками и связь с руководством оперативного орга-

на для скорейшей передачи управленческих решений и обеспечения их исполнения.

В условиях задержания с поличным от согласованности действий оперативников часто зависит успех всей операции и своевременное пресечение наступления возможных неблагоприятных последствий. При этом оперативному работнику важно хорошо знать возможности технических средств, обладать навыками работы на различных каналах, уметь пользоваться условными выражениями и знаками.

Среди технических средств, нашедших практически повседневное применение в работе оперативных работников (оперативников), особо выделяется аппаратура, предназначенная для приема, передачи и фиксации акустической информации, иначе говоря, средства оперативной звукозаписи. Сюда входят микрофоны различных типов, магнитофоны, диктофоны. Основное достоинство использования звукозаписи в ОРМ состоит в том, что она позволяет с достаточной полнотой и точностью фиксировать на магнитный носитель практически любую звуковую информацию.

Контроль и запись телефонных и иных переговоров граждан, несомненно, являются эффективным инструментом раскрытия преступлений. Вместе с тем прослушивание означает серьезное вторжение государства в частную жизнь граждан. Его можно легко использовать «не по назначению» — для установления тотального контроля за образом мыслей, высказываниями и взаимоотношениями людей. В этой связи задача законодателя видится в том, чтобы, не нанося ущерба качеству раскрытия преступлений, защитить частную жизнь граждан от незаконного и необоснованного вмешательства.

До 80-х годов прошлого столетия телефонные переговоры контролировались, в основном, спецслужбами. В период огульного разоблачения их деятельности, в открытой печати приводились данные о том, что до августа 1991 года 12-й отдел КГБ ежедневно записывал только по г. Москве около 300 абонентов, в основном иностранных граждан и преступников. Контроль служебных переговоров велся и на особо режимных объектах, но здесь следили не за конкретным человеком, а за утечкой информации с грифом «секретно». В таких случаях использовались специальные системы, работающие по «ключевым словам» и позволяющие прерывать (блокировать) телефонный разговор или отдельные фразы. Номера телефонов абонентов — нарушителей режима — устанавливались без затруднений при помощи специальной дорогостоящей аппаратуры. Поэтому использовалась она в основном в правительственных учреждениях и на объектах оборонной промышленности. Сейчас прослушивание и звукозапись телефонных переговоров ведется в совершенно иных социальных и технических условиях.

Прослушивание телефонных переговоров во времена тоталитарного режима применялось достаточно широко, хотя не было предусмотрено законом. Когда возник вопрос о легализации прослушивания, ряд авторитетных юристов высказались за его категорическое запрещение как недопустимое в демократическом обществе. Тем не менее, в 1990 году контроль телефонных переговоров получил в нашей стране законодательное обоснование. 12 июня 1990 г. был принят Закон СССР «О внесении изменений и дополнений в Основы уголовного судопроизводства Союза ССР и союзных республик». В соответствии с Основами телефонные переговоры можно было прослушивать на основании постановления органа дознания или следователя, санкционированного прокурором или судом. В дальнейшем право на прослушивание было закреплено за органами внутренних дел

(ОВД) и Федеральной службой безопасности (ФСБ) в Федеральных законах 1992 и 1995 года, затем право на оперативно-розыскную деятельность (ОРД), в том числе и на прослушивание, получили и другие органы, при наличии достаточных оснований полагать, что будет получена информация, имеющая существенное значение для расследования уголовного дела. Максимальный срок прослушивания составлял шесть месяцев. Оно могло также проводиться в случае угрозы противоправных действий в отношении свидетелей или потерпевших.

Закон об ОРД рассматривает прослушивание телефонных разговоров как одну из разновидностей ОРМ. Такие меры могут быть приняты только на основании судебного решения и при наличии информации:

1) о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно;

2) о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно;

3) о событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации (ст. 8 Закона об ОРД).

Практическое применение этого Закона вызывало серьезные сложности. С одной стороны, Основами был предусмотрен ряд условий производства этого следственного действия — необычного по своему содержанию из-за того, что сам следователь не участвует в прослушивании и звукозаписи телефонного разговора, а лишь организует это мероприятие и занимается процессуальным оформлением его результатов. С другой стороны, общесоюзный законодатель указал, что порядок прослушивания и звукозаписи определяется уголовно-процессуальным законодательством союзных республик. В УПК РСФСР на тот момент такая норма отсутствовала. Более того, высказывались сомнения по поводу самой возможности регламентации производства рассматриваемого следственного действия. Так, Г. Козырев полагает, что «производство следственного действия должно быть регламентировано от начала до конца. Обычно оно производится следователем с участием понятых и не может содержать никаких негласных, секретных аспектов. В данном же случае этот принцип соблюсти практически невозможно». Кроме того, процедура прослушивания телефонных переговоров неизбежно включает в себя организационные и тактические аспекты проведения ОРМ, которые должны носить закрытый характер.

Тем не менее, по мнению ряда процессуалистов, исключать регламентированное ст. 35.1 Основ прослушивание телефонных переговоров из числа следственных действий не следовало. Дело в том, что после распада СССР Основы уголовного судопроизводства формально отменены не были, а УПК РСФСР не содержал отдельной статьи, где были бы даны понятие и исчерпывающий перечень следственных действий. Следовательно, с точки зрения сторонников этой позиции, перечень следственных действий мог быть расширен за счет ст. 35.1 Основ.

По мнению А. Козусева, указанную статью следовало признать действующей на территории России еще и потому, что отсутствие такой нормы «ограничивает права следователя» и «уменьшает круг доказательств по уголовному делу». С подобными аргументами сложно согласиться — они делают возможности по расширению круга следственных действий практически неограниченными, что недопустимо с точки зрения охраны прав и свобод граждан.

Вместе с тем большинство авторов не включали прослушивание в число следственных действий. Оно не упоминалось даже при делении следственных действий на общепризнанные и не являющиеся таковыми. В 1998 г. И. Л. Петрухин высказал мнение, что прослушивание не будет предусмотрено в новом УПК РФ, поскольку «следователь может лишь вынести постановление о прослушивании и поручить его исполнение оперативно-розыскному органу. Сам же следователь с понятыми выполнить эту работу не в состоянии, так как она требует технических навыков и больших затрат времени».

Тем не менее в соответствии с Федеральным законом от 20 марта 2001 г. № 26-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с ратификацией Конвенции о защите прав человека и основных свобод» УПК РСФСР был дополнен ст. 174.1 «Контроль и запись переговоров» (см.: Норма аналогичного содержания и с таким же названием вошла и в новый УПК РФ // Российская газета. 2001. № 58. Ст. 186).

Термин «переговоры» в ст. 186 УПК РФ законодатель раскрывает как «телефонные и иные переговоры». Представляется, что понятие «иные переговоры» слишком неопределенно. Очевидно, законодатель имеет в виду не любые переговоры, а те, которые ведутся с помощью телекоммуникационных средств (видеотелефоны, компьютерные сети, спутниковая телесвязь и др.). В этой связи можно было бы использовать опыт зарубежных стран, например Франции, где соответствующий Закон называется «О перехвате сообщений, передаваемых с помощью средств телекоммуникации». Под телекоммуникациями понимается «всякая передача, перевод или прием любого рода знаков, сигналов, текстов, изображений, звуков или сведений с помощью оптического провода, радио, электричества или иных электронных систем».

Анализ ст. 186 УПК РФ позволяет выделить два этапа рассматриваемого следственного действия:

1) контроль и запись переговоров (проводится оперативными работниками по постановлению следователя, санкционированному судом);

2) осмотр и прослушивание фонограммы (осуществляется следователем с участием понятых).

По российскому законодательству контроль телефонных и иных переговоров представляет собой меру ограниченного применения. Прослушивание допустимо только по делам о тяжких и особо тяжких преступлениях (ч. 1 ст. 186 УПК РФ). На мой взгляд, принимая во внимание весьма существенное ограничение прав граждан при прослушивании и отсутствие у них возможности защитить эти права, закон следует дополнить положением о том, что данная мера может быть применена только при невозможности получить интересующие следствие сведения иными способами.

Части 1, 2 ст. 186 УПК РФ определяют, чьи переговоры и на каком основании могут быть записаны и прослушаны. Названных в законе субъектов можно разделить на две группы — в зависимости от их процессуального положения и целей, которые ставят при этом органы уголовного преследования:

а) обвиняемый, подозреваемый, иные лица — при наличии достаточных оснований полагать, что их телефонные и иные переговоры могут содержать сведения, имеющие значение для уголовного дела;

б) потерпевший, свидетель, их близкие родственники, родственники, близкие лица — при наличии угрозы совершения против них преступных действий.

В первом случае целью контроля и записи переговоров является получение доказательственной информации по делу; во втором — защита перечисленных лиц

от преступных посягательств. Различные цели определяют различные формальные основания контроля переговоров. В первом случае следователю необходимо получить решение суда, во втором — заявление указанных лиц либо — при отсутствии такого заявления — решение суда.

Применительно к субъектам первой группы представляется необходимым конкретизировать понятие «сведения, имеющие значение для уголовного дела». В противном случае прослушивание может стать инструментом для сбора любой информации, характеризующей личность обвиняемого (подозреваемого), что недопустимо. Думается, что фактическими основаниями контроля переговоров названной категории лиц могут быть: получение доказательственной информации о преступлении, его участниках, местах сокрытия орудий и объектов преступной деятельности; розыск скрывшегося обвиняемого (подозреваемого).

Максимальный срок производства контроля и записи телефонных и иных переговоров составляет 6 месяцев. Прослушивание прекращается, когда необходимость в данной мере отпадает, но не позднее окончания срока предварительного расследования по данному уголовному делу (ч. 5 ст. 186 УПК РФ).

В соответствии с ч. 7 ст. 186 УПК РФ в осмотре и прослушивании фонограммы принимают участие понятые. На мой взгляд, целесообразно дополнить УПК правилом о необходимости предупреждения лиц, присутствующих при прослушивании, об уголовной ответственности за нарушение тайны телефонных переговоров по ст. 138 УК РФ.

Важной гарантией неразглашения содержания телефонных переговоров является требование ч. 8 ст. 186 УПК РФ, согласно которому фонограмма должна храниться в опечатанном виде в условиях, исключающих возможность прослушивания и тиражирования фонограммы посторонними лицами.

Таким образом, следует признать, что современное российское уголовно-процессуальное законодательство в части прослушивания телефонных и иных переговоров в целом отвечает мировым стандартам.

Итак, контроль и запись переговоров — мощный инструмент, позволяющий эффективно расследовать преступления, но в то же время создающий повышенную угрозу неприкосновенности частной жизни в силу следующих причин:

а) гражданин, как правило, не подозревает о таком вмешательстве в его частную жизнь и, следовательно, лишен возможности обжаловать действия следователя;

б) прослушивание неизбирательно: прослушиваются все разговоры подряд, пока не будут получены интересующие следствие сведения, что влечет за собой достаточно глубокое проникновение в сферу частной жизни граждан;

в) как отмечено выше, сама процедура прослушивания не может быть полностью «прозрачной»: она обязательно содержит организационные и тактические аспекты, которые носят закрытый характер, что создает значительные возможности для злоупотреблений со стороны правоохранительных органов.

В этой связи необходимы повышенные гарантии законности действий следователя, касающиеся как оснований, так и процедуры контроля переговоров. В законе максимально четко должны быть определены: категории дел, по которым допустимо применение данной меры; субъекты, чьи телефоны могут быть подвергнуты прослушиванию; фактические и формальные основания его производства; процессуальный порядок проведения данного следственного действия и фиксации его результатов; дальнейшая судьба материалов, полученных в результате прослушивания.

§ 3. Полиграф, детектор лжи

Велась, да и сейчас ведется дискуссия широкого использования технических возможностей полиграфа — детектора лжи. Этот прибор давно применяется во многих странах мира. В нашей стране долгое время скрывали фактическое использование полиграфа в работе специальных подразделений правоохранительных органов, поскольку это не предусматривалось действующим законодательством.

Известно, что полиграф — это психофизический регистратор реакций человека. Его работа основывается на непрерывном измерении кровяного давления, частоты пульса, влажности кожного покрова и некоторых других изменяющихся объективных параметров. При возникновении внутреннего напряжения (например, при воспроизведении ложных показаний) показатели этих состояний существенно отличаются от нормальных. Специальная методика оценки результатов измерений, сделанных на полиграфе, позволяет прийти к выводу о степени истинности показаний.

Полиграф представляет собой совокупность диагностических приборов, широко используемых в медицине. С помощью специальных датчиков, установленных на теле человека, способен регистрировать свыше двадцати параметров жизнедеятельности организма. Датчики фиксируют различные изменения, вызываемые эмоциональным откликом на происходящие события. Основным принципом тестирования на полиграфе является то, что человек, умышленно скрывающий или искажающий информацию, испытывает внутренний дискомфорт. Чем выше значимость известной ему информации, тем больше динамика психофизиологических реакций организма.

В оперативно-розыскной деятельности результаты «полиграфных» проверок могут служить лишь ориентирующей информацией, не имеющей доказательственного значения, а, следовательно, в дальнейшем не могут использоваться в суде. Ценность таких результатов во многом зависит от характера вопросов, относящихся к расследуемому преступлению. Полиграф помогает определить направление поиска, уточнить или обнаружить некоторые, интересующие оперативных работников (оперативников), данные. По общему правилу любые сомнения в правильности выводов о наблюдаемой реакции должны трактоваться в пользу проверяемого.

Вначале детектор лжи применялся оперативно-розыскными службами лишь в порядке эксперимента для раскрытия наиболее тяжких или вызвавших большой общественный резонанс преступлений. Ныне его использование разрешается и подробно регламентируется ведомственными нормативными актами ФСБ и МВД.

Предусматривается, что проверка граждан на детекторе лжи осуществляется только с добровольного согласия или по просьбе проверяемых лиц, которые вправе в любой момент прервать ее проведение. Однако результаты проведенного тестирования не могут заменять доказательств, полученных процессуальным путем, являться основанием для предъявления обвинения. Отказ от такой проверки не должен повлечь отрицательных последствий, усиливать подозрения о причастности проверяемого к противоправным действиям.

В оперативно-розыскной деятельности зарубежных стран проверки на детекторе лжи, как правило, используются не в интересах полученных судебных доказательств, а для оказания содействия официальному расследованию. Так, в США Верховный суд более тридцати лет назад признал — любое принуждение к испытанию на полиграфе является грубым нарушением прав человека. Испытание на детекторе

лжи должно проводиться только с письменного согласия испытуемого и с санкции органов, осуществляющих уголовное преследование. Применение полиграфа четко регламентировано не только федеральным законодательством, но и законодательством отдельных штатов.

По российскому законодательству данные, полученные при помощи полиграфа, также не являются доказательствами, а имеют характер оперативных данных. Хотя в будущем, не исключено, что качество и количество произведенных проверок повлечет за собой изменения в статусе полиграфных обследований. Эта процедура может быть отнесена к категории судебно-психофизиологической экспертизы. Оператор полиграфа, как лицо, обладающее специальными знаниями и навыками, может наделяться процессуальными правами и обязанностями специалиста.

Технология полиграфа такова, что может представлять интерес для диагностики и формирования высокой корпоративной культуры оперативных подразделений. Экстремальные условия, в которых приходится работать оперативнику, предъявляют повышенные требования к профессиональной пригодности и надежности. Среди факторов, оказывающих определенное влияние на надежность, можно выделить уровень материального положения, несовершенство законодательства, инертность мышления и др. В такой ситуации с помощью полиграфа можно обследовать экономическую, социально-политическую и морально-психологическую стороны деятельности сотрудников, работающих в одном коллективе, сформировав соответствующий банк данных. Изученные аспекты будут, таким образом, охватывать практически все области наиболее значимых мотивов действий каждого оперативного работника, через выяснение его ценностной ориентации и психологических установок.

Полиграф «ЭПОС-7». Полиграф предназначен для проведения оценки подготовленным специалистом достоверности информации, сообщаемой тестируемым лицом, а также для оценки уровня эмоциональной напряженности.

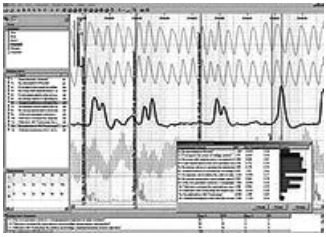
Компьютерный полиграф ЭПОС-7 является дальнейшим развитием полиграфных систем серии ЭПОС, впервые вышедших на рынок в 1996 году. К настоящему времени полиграфы серии ЭПОС успешно функционируют в более чем 200 центрах психофизиологического тестирования МВД, Минобороны, Минюста, ФПС России, других федеральных ведомствах, показав свою высокую эффективность.

Программа для полиграфа ЭПОС-7 является 32-битным приложением только для Windows 95, 98, 2000, XP и не требует от оператора специальных навыков работы с компьютером, кроме тех, которые необходимы для работы в среде Windows.

Профессиональный компьютерный ***полиграф «Диана-01»,*** реализующий аппаратурный метод детекции лжи.

ПКП «Диана-01» применяется в оперативно-розыскной и кадровой работе, в ходе служебных разбирательств по фактам злоупотреблений, хищений, а также для выявления у человека возможно скрываемой им информации.

Технические особенности



– Использование алгоритма ChanceCalc обеспечивает вычисление вероятности неслучайности реакций на предъявляемые стимулы.

– Наличие специализированной Стресс-шкалы позволяет оценить относительный уровень стресса обследуемого непосредственно в процессе тестирования.

– Интеллектуальная настройка регистрируемых сигналов позволяет поддерживать вид записываемой полиграммы в соответствии с заранее спроектированным шаблоном.

– Возможно хранение и оперативный поиск проведенного обследования как по тексту, так и по времени тестирования, записанного в стандартной базе данных.

В полиграфе использован компактный, прочный и электробезопасный корпус с защитой от излучений мобильных телефонов и других устройств.

Основные характеристики

Полиграф обеспечивает отображение в графическом виде следующих физиологических показателей человека:

- фазическая составляющая кожно-гальванической реакции (одновременно до 2 каналов);
- тоническая составляющая кожно-гальванической реакции;
- плетизмограмма (регистрация работы сердца через периферические кровеносные сосуды);

- артериальное давление;
- регистрация изменения объема груди;
- регистрация изменения объема живота;
- регистрация мимики лица и общей активности мышц тела испытуемого;
- регистрация речевого сигнала;
- регистрация частоты сердечных сокращений.

§ 4. Противодействие техническим средствам разведки

Противодействие техническим средствам разведки (ТСР) представляет собой совокупность согласованных мероприятий, предназначенных для исключения или существенного затруднения добывания охраняемых сведений с помощью технических средств.

Добывание информации предполагает наличие информационных потоков от физических носителей охраняемых сведений к системе управления. При использовании ТСР такие информационные потоки образуются за счет перехвата и анализа сигналов и полей различной физической природы. Источниками информации для технической разведки являются содержащие охраняемые сведения объекты. Это позволяет непосредственно влиять на качество добываемой злоумышленником информации и в целом на эффективность его деятельности путем скрытия истинного положения и навязывания ложного представления об охраняемых сведениях.

Искажение или снижение качества получаемой информации непосредственно влияет на принимаемые злоумышленником решения и, через его систему управления, на способы и приемы исполнения решения. Непосредственный контакт принципиально необходим на этапах добывания информации и исполнения решения, причем добывание информации должно предшествовать принятию решения и его исполнению злоумышленником. Поэтому противодействие ТСР должно носить упреждающий характер и реализовываться заблаговременно.

Любая система технической разведки содержит следующие основные элементы (рис. 5.4.1):

- технические средства разведки (ТСР);
- каналы передачи информации (КПИ);
- центры сбора и обработки информации (ЦСОИ).

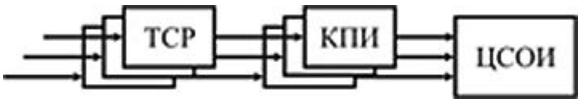


Рисунок 5.4.1 — Упрощенная структурная схема системы технической разведки

Технические средства разведки представляют собой совокупность разведывательной аппаратуры, предназначенной для обнаружения демаскирующих признаков, предварительной обработки, регистрации перехваченной информации и ее передачи через КПИ в ЦСОИ. В ЦСОИ информация от различных ТСР накапливается, классифицируется, анализируется и предоставляется потребителям (автоматизированным системам управления или лицам, принимающим решения. Таким образом, в системе технической разведки реализуется обнаружение и анализ демаскирующих признаков (ДП).

Обнаружение ДП по физической сути заключается в выполнении следующих операций:

– поиск и обнаружение энергии ДП в пространстве, во времени, по спектру и т. д.;
– выделение ДП из искусственных и естественных помех.

Физический смысл анализа ДП раскрывают следующие операции:

– разделение ДП различных объектов;
– оценка параметров ДП (определение их объективных характеристик);
– сокращение избыточности информации;
– регистрация, накопление и классификация ДП;
– нахождение местоположения источника ДП;
– распознавание смыслового содержания ДП;
– выявление охраняемых сведений.

В соответствии с приведенной классификацией главными направлениями снижения эффективности ТСР является противодействие обнаружению ДП и противодействие их анализу.

При противодействии обнаружению ДП преследуется цель скрытия от ТСР демаскирующих признаков. Соответственно все организационные и технические способы, предназначенные для исключения или существенного затруднения обнаружения ДП, составляют одно из главных направлений противодействия ТСР — скрытие.

Другим основным направлением является техническая дезинформация, которая объединяет все организационно-технические меры противодействия, направленные на затруднение анализа ДП и навязывание противнику ложной информации.

Скрытие, обеспечивая противодействие обнаружению, всегда затрудняет или исключает возможность проведения анализа демаскирующего признака. Техническая дезинформация, наоборот, затрудняя анализ, как правило, не влияет на возможность обнаружения объекта разведки.

Некоторые ТСР предназначены для обеспечения активного воздействия на любые объекты, чьи сигналы оказываются в заданных диапазонах поиска и обнаружения. Техническая дезинформация в такой ситуации может оказаться неэффективной. Поэтому реализация стратегии скрытия объекта является более радикальным направлением противодействия ТСР, чем техническая дезинформация.

Однако на практике часто встречаются ситуации, когда невозможно обеспечить при ограниченных ресурсах надежное скрытие объекта (например, крупного здания или сооружения) или отдельных демаскирующих признаков (таких, как мощные непрерывные электромагнитные излучения радиоэлектронных и оптических систем на открытой местности). В подобных ситуациях цели противодействия техническим средствам разведки могут достигаться только применением методов и средств технической дезинформации.

Кроме рассмотренных мер ПД ТСР, предполагающих нормальное функционирование всех составных частей системы разведки, возможно проведение активных действий по выявлению и выведению из строя элементов системы разведки.

Основными функциями системы разграничения доступа (СРД) являются:

– реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

– реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

– изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

– управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

– реализация правил обмена данными между субъектами для автоматизированных систем (АС) и средств вычислительной техники, построенных по сетевым принципам.

Функционирование СРД опирается на выбранный способ разграничения доступа. Наиболее прямой способ гарантировать защиту данных — это предоставить каждому пользователю вычислительную систему как его собственную. В многопользовательской системе похожих результатов можно добиться использованием модели виртуальной ЭВМ.

При этом каждый пользователь имеет собственную копию операционной системы. Монитор виртуального персонального компьютера для каждой копии операционной системы будет создавать иллюзию, что никаких других копий нет и что объекты, к которым пользователь имеет доступ, являются только его объектами. Однако при разделении пользователей неэффективно используются ресурсы АС.

В АС, допускающих совместное использование объектов доступа, существует проблема распределения полномочий субъектов по отношению к объектам. Наиболее полной моделью распределения полномочий является матрица доступа. Матрица доступа является абстрактной моделью для описания системы предоставления полномочий.

Строки матрицы соответствуют субъектам, а столбцы — объектам; элементы матрицы характеризуют право доступа (читать, добавлять информацию, изменять информацию, выполнять программу и т. д.). Чтобы изменять права доступа, модель может, например, содержать специальные права владения и управления. Если субъект владеет объектом, он имеет право изменять права доступа других субъектов к этому объекту. Если некоторый субъект управляет другим субъектом, он может удалить права доступа этого субъекта или передать свои права доступа этому субъекту. Для того чтобы реализовать функцию управления, субъекты в матрице доступа должны быть также определены в качестве объектов.

Элементы матрицы установления полномочий (матрицы доступа) могут содержать указатели на специальные процедуры, которые должны выполняться при каждой попытке доступа данного субъекта к объекту и принимать решение о возможности доступа. Основами таких процедур могут служить следующие правила:

– решение о доступе основывается на истории доступов других объектов;

– решение о доступе основывается на динамике состояния системы (права доступа субъекта зависят от текущих прав других субъектов);

– решение о доступе основывается на значении определенных внутрисистемных переменных, например, значений времени и т. п.

В наиболее важных АС целесообразно использование процедур, в которых решение принимается на основе значений внутрисистемных переменных (время доступа, номера терминалов и т. д.), так как эти процедуры сужают права доступа.

Матрицы доступа реализуются обычно двумя основными методами — либо в виде списков доступа, либо мандатных списков. Список доступа приписывается каждому объекту, и он идентичен столбцу матрицы доступа, соответствующей этому объекту. Списки доступа часто размещаются в словарях файлов. Мандатный список приписывается каждому субъекту, и он равносилен строке матрицы доступа, соответствующей этому субъекту. Когда субъект имеет права доступа по отношению к объекту, то пара (объект — права доступа) называется мандатом объекта.

На практике списки доступа используются при создании новых объектов и определении порядка их использования или изменении прав доступа к объектам.

С другой стороны, мандатные списки объединяют все права доступа субъекта. Когда, например, выполняется программа, операционная система должна быть способна эффективно выявлять полномочия программы. В этом случае списки возможностей более удобны для реализации механизма предоставления полномочий.

Некоторые операционные системы поддерживают как списки доступа, так и мандатные списки. В начале работы, когда пользователь входит в сеть или начинает выполнение программы, используются только списки доступа. Когда субъект пытается получить доступ к объекту в первый раз, список доступа анализируется и проверяются права субъекта на доступ к объекту. Если права есть, то они приписываются в мандатный список субъекта и права доступа проверяются в дальнейшем проверкой этого списка.

При использовании обоих видов списков список доступа часто размещается в словаре файлов, а мандатный список — в оперативной памяти, когда субъект активен. С целью повышения эффективности в техническом обеспечении может использоваться регистр мандатов.

Третий метод реализации матрицы доступа — так называемый механизм замков и ключей. Каждому субъекту приписывается пара (A, K), где A — определенный тип доступа, а K — достаточно длинная последовательность символов, называемая замком. Каждому субъекту также предписывается последовательность символов, называемая ключом. Если субъект захочет получить доступ типа A к некоторому объекту, то необходимо проверить, что субъект владеет ключом к паре (A, K), приписываемой конкретному объекту.

К недостаткам применения матриц доступа со всеми субъектами и объектами доступа можно отнести большую размерность матриц. Для уменьшения размерности матриц установления полномочий применяют различные методы сжатия:

– установление групп пользователей, каждая из которых представляет собой группу пользователей с идентичными полномочиями;

– распределение терминалов по классам полномочий;

– группировка элементов защищаемых данных в некоторое число категорий с точки зрения безопасности информации (например, по уровням конфиденциальности).

По характеру управления доступом системы разграничения разделяют на дискреционные и мандатные.

Дискреционное управление доступом дает возможность контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам и т. п.). Например, владельцам объектов предоставляется право ограничивать доступ к этому объекту других пользователей. При таком управлении доступом для каждой пары (субъект-объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), т. е. тех типов доступа, которые являются санкционированными для данного субъекта к данному объекту. Однако имеются и другие задачи управления доступом, которые не могут быть решены только дискреционным управлением. Одна из таких задач — позволить администратору АС контролировать формирование владельцами объектов списков управления доступом.

Мандатное управление доступом позволяет разделить информацию на некоторые классы и управлять потоками информации при пересечениях границ этих классов.

Во многих системах реализуется как мандатное, так и дискреционное управление доступом. При этом дискреционные правила разграничения доступа являются дополнением мандатных. Решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционны-

ми, и мандатными ПРД. Таким образом, должны контролироваться не только единичный акт доступа, но и потоки информации.

Обеспечивающие средства для системы разграничения доступа выполняют следующие функции:

– идентификацию и опознавание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

– регистрацию действий субъекта и его процесса;

– предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

– реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление системы защиты после НСД;

– тестирование всех функций защиты информации специальными программными средствами;

– очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными путем двукратной произвольной записи;

– учет выходных печатных и графических форм и твердых копий в АС;

– контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Для каждого события должна регистрироваться следующая информация, дата и время; субъект, осуществляющий регистрируемое действие; тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа); успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выдача печатных документов должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе общего количества листов (страниц). Вместе с выдачей документа может автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа.

Автоматическому учету подлежат создаваемые защищаемые файлы, каталоги, тома, области оперативной памяти персонального компьютера, выделяемые для обработки защищаемых файлов, внешних устройств и каналов связи.

Такие средства, как защищаемые носители информации, должны учитываться документально, с использованием журналов или картотек, с регистрацией выдачи носителей. Кроме того, может проводиться несколько дублирующих видов учета.

Реакция на попытки НСД может иметь несколько вариантов действий:

– исключение субъекта НСД из работы АС при первой попытке нарушения ПРД или после превышения определенного числа разрешенных ошибок;

– работа субъекта НСД прекращается, а информация о несанкционированном действии поступает администратору АС и подключает к работе специальную программу работы с нарушителем, которая имитирует работу АС и позволяет администрации сети локализовать место попытки НСД.

Реализация системы разграничения доступа может осуществляться как программными, так и аппаратными методами или их сочетанием. В последнее время аппаратные методы защиты информации от НСД интенсивно развиваются благодаря тому, что: во-первых, интенсивно развивается элементная база, во-вторых, стоимость аппаратных средств постоянно снижается и, наконец, в-третьих, аппаратная реализация защиты эффективнее по быстродействию, чем программная.

Тема 6. СПЕЦИАЛЬНЫЕ ХИМИЧЕСКИЕ ВЕЩЕСТВА

§ 1. Виды специальных химических веществ и их основные свойства

Специальные химические вещества (СХВ)в зависимости от свойств, условий применения и способов обнаружения условно можно разделить на следующие группы: красящие, люминесцирующие (органического происхождения — люминофоры, неорганического происхождения — светосоставы), индикаторы и запаховые вещества.

Красящие вещества — это химические вещества, обеспечивающие стойкое окрашивание контактирующих поверхностей и преимущественно применяемые для активного выявления, изобличения лиц, совершающих кражи.

При попадании на открытые части тела человека, его одежду, на другие предметы они под воздействием потожировых выделений или окружающей влаги растворяются и образуют ярко окрашенные пятна. Это создает своего рода «особые приметы». Устранить такие пятна очень сложно. На поверхности тела, например, они остаются после многократного смывания горячей водой с моющими средствами, особенно под ногтями и в складках кожи. С одежды и других предметов удалить полностью красящие вещества практически невозможно. Следует учитывать, что некоторые из них обладают способностью люминесцировать в ультрафиолетовых лучах. Это позволяет выявлять такие вещества и в тех случаях, когда обычным осмотром они не обнаруживаются из-за малого количества или маскировки на объекте за счет сходства окраски.

Красящие вещества гигроскопичны, т.е. обладают способностью впитывать в себя влагу из окружающего воздуха. Это явление крайне нежелательно, т.к. порошкообразные красящие вещества, впитав влагу, во-первых, теряют свои свойства и при повторном увлажнении окрашивают контактирующую поверхность недостаточно стойко, а, во-вторых, подвергшись увлажнению, могут окрасить и демаскировать помеченный объект. Так, следы увлажненного и затем высушенного родамина С легко удаляются с рук простым мытьем водой с мылом. Поэтому при хранении и применении красящих веществ во избежание порчи и для увеличения срока годности последних необходимо исключать их контакт с влагой и влажным воздухом.

После срабатывания ловушки следы СХВ могут быть обнаружены по характерной окраске, заметной невооруженным глазом, и по люминесценции в ультрафиолетовых лучах. Экспертные исследования базовых смесей проводятся методом тонкослойной хроматографии и идентификации красителей и других компонентов путем сравнения с эталонами и при помощи цветных реакций, проводимых капельным способом непосредственно на пластинке.

Для исследования СХВ ведьма удобны различные методы молекулярной спектроскопии, в частности спектрофотометрия. Определение цветовых спектральных характеристик этих веществ проводят на регистрирующих спектрофотометрах.

Красящие вещества, используемые в работе ОВД, обладают следующими свойствами:

Родамин С — темно-коричневый порошок с зеленоватым оттенком. Растворы в воде и спирте имеют синевато-красную окраску. Контактирующую поверхность

при увлажнении окрашивает в стойкий малиновый цвет. В ультрафиолетовых лучах имеет ярко-красную люминесценцию.

Родамин Ж — красный или желто-коричневый порошок. Растворим в воде и спирте. Образующиеся растворы имеют ярко-красную окраску и зеленовато-желтую люминесценцию. Контактирующую поверхность окрашивает в коричнево-красный цвет с ярко-желтой люминесценцией в ультрафиолетовых лучах.

Родамин 4С — темно-малиновые кристаллы. Раствор в воде имеет темно-малиновую окраску, в этиловом спирте — розовато-малиновую. Контактирующую поверхность при увлажнении окрашивает в розово-малиновый цвет, люминесцирует таким же цветом.

Основной ярко-зеленый — порошок зеленого цвета с золотистым блеском. Контактирующую поверхность окрашивает в стойкий зеленый цвет. Плохо растворяется в воде, растворим в спирте.

Метиленовый голубой — вещество темно-зеленого цвета. Контактирующую поверхность окрашивает в ярко-голубой цвет. В воде и спирте растворяется плохо, но при нагревании растворимость улучшается. Растворы имеют синюю окраску.

Хризоидин — порошок красно-коричневого цвета. Контактирующую поверхность окрашивает в желто-оранжевый цвет. Слабо растворим в воде и хорошо — в этиловом спирте, диэтиловом эфире, хлороформе. Растворы имеют оранжево-коричневую окраску.

Сафранин Т — коричнево-красный порошок. Окрашивает контактирующую поверхность в красный цвет. Растворим в воде и спирте. В ультрафиолетовых лучах при увлажнении этиловым спиртом имеет красную люминесценцию.

Метилвиолет (метиленовый фиолетовый) — порошок с зеленым металлическим блеском. Растворы в воде и этиловом спирте имеют фиолетовую окраску.

Нейтральный красный — темно-зеленый кристаллический порошок. Водный раствор имеет красную окраску. Раствор в этиловом спирте красного цвета, слегка люминесцирует малиново-красным цветом.

Нильский синий — зеленый кристаллический порошок с бронзовым блеском. Плохо растворим в холодной воде, при нагревании растворимость повышается. Растворим в этиловом спирте. Растворы окрашены в синий цвет.

Фуксин основной — темно-зеленые блестящие кристаллы. Контактирующую поверхность окрашивает в розовый цвет. Растворим в воде (лучше при нагревании), хорошо растворим в этиловом спирте. Растворы имеют розовую окраску.

Основной синий К — порошок синего цвета. Контактирующую поверхность окрашивает в синий цвет. Растворим в воде и этиловом спирте. Растворы имеют синюю окраску.

Основной, коричневый 2К — черно-коричневый порошок. Растворы в воде и этиловом спирте имеют коричневую окраску.

Азур 1 (метиленазур) — темно-коричневые кристаллы с зеленоватым блеском. Растворим в воде, хорошо растворим в метиловом и этиловом спирте. Растворы имеют синюю окраску. Спиртовые растворы обладают синевато-красной люминесценцией.

Бриллиантовый желтый — светло-коричневый порошок. Растворы в воде и этиловом спирте имеют желто-оранжевую окраску.

Эозин — желтовато-оранжевый кристаллический порошок. Не растворим в воде и бензоле; плохо растворим в этиловом спирте, хорошо — в щелочах. Образующиеся растворы имеют розовую окраску.

Люминесцирующие вещества — химические вещества, обладающие способностью люминесцировать (светиться) в ультрафиолетовых лучах.

Некоторые вещества обладают способностью при освещении не только отражать часть падающего на них света, но и начинают светиться сами, особенно под действием источников, испускающих ультрафиолетовый свет.

Явление холодного свечения некоторых химических веществ строго определенным цветом при освещении их ультрафиолетовыми лучами называется фотолюминесценцией (сочетание греческого слова «фотос» — свет и латинского «люминесценция» — свечение). Согласно правилу Стокса свет люминесценции характеризуется большей длиной волны, чем возбуждающий свет. Поэтому при освещении вещества оно может люминесцировать специфичным именно для него цветом.

Обращает на себя внимание тот факт, что некоторые вещества сохраняют способность светиться определенное время после того, как освещение прекратилось (остаточное послесвечение). Эта разновидность фотолюминесценции названа фосфоресценцией. Свечение, которое прекращается вместе с освещением, называется флюоресценцией. Однако резкую границу между ними провести трудно и деление это до известной степени условно.

Явление люминесценции применяется для люминесцентного анализа. Используемые в работе ОВД люминесцирующие вещества являются, как правило, бесцветными или слабоокрашенными. Кроме того, порошкообразные люминесцирующие вещества мелкодисперсны и обладают хорошими адгезионными свойствами. Благодаря этому они находят широкое применение при проведении ОРМ для скрытой пометки каких-либо объектов. Явление люминесценции дает возможность выявить присутствие ничтожно малых количеств люминесцирующих веществ. Например, достаточно располагать миллионной долей грамма светящегося вещества в виде раствора, чтобы обнаружить его по характерной люминесценции.

Основные представители люминесцирующих веществ, используемые в ОВД, обладают следующими свойствами:

Светосостав БЗС — мелкокристаллический белый порошок. В воде и других растворителях не растворяется. В ультрафиолетовых лучах светосостав БЗС имеет ярко-голубую люминесценцию. Используют это вещество для нанесения меток на ткань, пряжу, мех.

Светосостав ФК-102 — желто-оранжевый мелкокристаллический порошок. Нерастворим в воде и других растворителях. В ультрафиолетовых лучах имеет оранжево-красную люминесценцию. Используется для нанесения меток на ткань, мех, пряжу.

Люмоген желто-зеленый — представляет собой аморфное вещество желто-зеленого цвета. Растворяется в органических растворителях, таких как толуол, дихлорэтан, бензин. В ультрафиолетовых лучах имеет желто-зеленую люминесценцию.

Люмоген водно-голубой — порошок бледно-голубого цвета. Хорошо растворяется в толуоле, бензине, дихлорэтане. В ультрафиолетовых лучах имеет голубую люминесценцию.

Люмоген светло-зеленый — мелкокристаллический порошок светло-зеленого цвета. Растворяется в толуоле, бензине, дихлорэтане. В ультрафиолетовых лучах имеет зеленую люминесценцию.

Прямой белый — белое порошкообразное вещество. В ультрафиолетовых лучах имеет голубую люминесценцию.

Риванол — представляет собой мелкокристаллический порошок желтого цвета. В воде растворяется плохо, но хорошо в спирте. В ультрафиолетовых лучах обладает желтой люминесценцией.

Тетрациклин — порошок желтого цвета. Плохо растворяется в воде. В ультрафиолетовых лучах имеет желтую люминесценцию.

Трифенилпиразолин — белый порошок. Растворим в спирте. В ультрафиолетовых лучах имеет голубую люминесценцию.

Следует отметить, что из всех перечисленных люминесцирующих веществ риванол, тетрациклин и трифенилпиразолин являются медицинскими препаратами. Это дает возможность использовать их для маркировки пищевых продуктов, т. к. в применяемых количествах, даже попав в организм человека, они не приносят вреда здоровью. Кроме того, эти вещества не влияют на вкусовые и питательные свойства помечаемых продуктов.

Индикаторы — это химические вещества, которые под воздействием определенных химических реактивов изменяют свой цвет. Они применяются для нанесения на объекты пометок, невидимых в обычных условиях, но легко обнаруживаемых за счет изменения окраски.

В работе ОВД в качестве индикаторов применяются медицинские препараты. Эти вещества безвредны для человека и окружающей среды. Индикаторы на основе медицинских препаратов просты в изготовлении и удобны для негласной маркировки и последующего обнаружения (проявления). Учитывается также, что вероятность случайного попадания фармацевтических препаратов на поверхность маркируемого предмета весьма мала.

Одним из представителей этой группы веществ является фенолфталеин.

Фенолфталеин — мелкозернистый порошок белого цвета. В воде растворяется плохо, но хорошо в спирте. Раствор фенолфталеина бесцветен и прозрачен. При добавлении к нему раствора со щелочной реакцией (например, раствора аммиака, соды и др.) приобретает ярко-малиновую окраску. Именно это его свойство и используется при проведении ОРМ.

В качестве индикаторов могут быть применены и другие фармацевтические препараты, например, салициловая кислота, антипирин, амидопирин, резерцин, глюконат кальция, анальгин, для проявления записей и пометок, произведенных растворами этих веществ, используют 3 % водный раствор хлорида железа (Ш).

Салициловая кислота — мелкие игольчатые кристаллы без запаха, белого цвета, при осторожном нагревании возгоняются (переходят в газообразное состояние, минуя жидкое). В воде салициловая кислота плохо растворима, легко растворяется в этиловом спирте, диэтиловом эфире. Образующиеся растворы бесцветны. При проявлении 3 % раствором FeCl3 приобретают фиолетовое окрашивание.

Антипирин — бесцветные кристаллы или белый кристаллический порошок без запаха, слабо-горького вкуса. Легко растворим в воде и этиловом спирте. Образующиеся растворы бесцветны. При воздействии раствором FeCl3 приобретают коричневое окрашивание.

Амидопирин — белые кристаллы или белый порошок без запаха, слабо-горького вкуса. Растворим в воде и этиловом спирте. Образующиеся растворы бесцветны. При воздействии раствором FeCl3 приобретают розовое окрашивание с коричневым оттенком.

Резорцин — белый или белый со слабым желтоватым оттенком кристаллический порошок, обладающий специфическим запахом. Под влиянием воздуха и света постепенно окрашивается в розовый цвет. Легко растворим в воде и этиловом спирте. Образующиеся растворы бесцветны. При воздействии раствором FeCl3 приобретают розовое окрашивание с бурым оттенком.

Глюконат кальция — белый зернистый кристаллический порошок без запаха и вкуса. Нерастворим в этиловом спирте. Растворим в воде. Образующийся раствор бесцветен. При воздействии раствором FeCl3 приобретает зеленовато-желтое окрашивание.

Анальгин — совсем белый или с едва желтоватым оттенком кристаллический порошок без запаха, горького вкуса. В воде растворим. Образующийся раствор бесцветен. При воздействии раствором FeCl3 окрашивается в розовый цвет с малиновым оттенком. Поскольку анальгин в присутствии влаги быстро разлагается, водный раствор его при хранении желтеет. Для маркировки объектов следует применять только свежеприготовленный раствор.

Перечисленные индикаторы являются медицинскими препаратами, что позволяет эффективно использовать их не только для маркировки различных предметов, но и пищевых продуктов.

При использовании фармацевтических препаратов для приготовления индикаторных растворов можно брать готовые лекарственные формы, содержащие исходные вещества, или готовые растворы предлагаемых фармацевтических препаратов,

Запаховые вещества — это специальные химические вещества, основным свойством которых является характерный стойкий запах, легко улавливаемый специально обученной собакой. В качестве этих веществ используют, как правило, мало распространенные природные химические соединения, которые обладают специфическим воздействием на обоняние и центральную нервную систему собаки. Запаховые препараты облегчают работу служебно-розыскных собак при проведении различных оперативных мероприятий.

На вооружении ОВД находятся следующие запаховые препараты: УС (усилитель следа) и СП-80 мс.

Препарат УС представляет собой специальным образом приготовленное порошкообразное вещество. Его запах хорошо распознается собаками в интервале температур от –20 до +30 °С. Следы препарата на одежде, обуви, предметах обихода легко обнаруживаются собакой в течение 3–7 дней. Для выборки предметов со следами УС пригодны обычные служебно-розыскные собаки, прошедшие непродолжительную специальную тренировку. УС может быть использован совместно с красящими и люминесцирующими веществами.

Препарат СП-80 мс — маслянистое вязкое вещество коричневого цвета с характерным запахом, слабо растворимое в воде, безвредное для человека и животных. Препарат состоит из жировой основы и специального пахучего вещества. В него добавлены люминесцирующие вещества. В некоторых случаях он используется без добавки последних. Эта его разновидность носит название СП-80.

Запах препарата в различных климатических условиях сохраняется на помеченных объектах (местности) до 10 суток. Препарат стоек к воздействию солнечных лучей, дождя, ветра, колебаний температуры воздуха.

Наличие его следов могут воспринимать собаки любых пород (служебно-розыскные, охотничьи, декоративные), у которых выработан комплекс условных рефлексов на этот препарат. Для поддержания рефлекса требуется лишь 2–3 тренировки в месяц.

Применение запаховых веществ предполагает создание таких условий, при которых обеспечивается перенесение их на обувь преступника. Это позволяет не только успешно отработать след, но и произвести выборку лиц, подозреваемых в совершении преступления. Пометка запаховым веществом различных материальных ценностей позволяет эффективно осуществлять их обнаружение и произ-

водить выборку помеченных объектов из ряда однородных. Сочетание запаховых веществ с красящими и люминесцирующими взаимно повышает эффективность их применения, т. к. позволяет выявлять соответствующие следы в течение длительного времени.

§ 2. Основные направления использования специальных химических веществ

СХВ применяются как для нанесения пометок на различные объекты во время проведения оперативных мероприятий, так и для снаряжения химических ловушек, устанавливаемых на объектах, где возможны или имеют место хищения.

В оперативно-розыскной деятельности специальные химические вещества используются в виде порошков, спецмазей, растворов, спецкарандашей, аэрозолей.

Вид СХВ, его агрегатное состояние выбираются исходя из складывающейся оперативной обстановки.

При этом учитываются характер, цвет предмета и условия его хранения. Перед тем как наносить метки на объекты, необходимо предварительно испытать химические вещества на образцах, аналогичных используемому материалу, и только после получения положительных результатов приступать к нанесению меток.

Порошкообразные СХВ применяются как отдельно, так и в смеси друг с другом. Они используются для пометки различных предметов с ворсистой или шероховатой поверхностью, а также для снаряжения устройств, обеспечивающих их распыление. Как правило, это смеси красящих и люминесцирующих веществ.

Порошки СХВ наносят с помощью кисточки или путем насыпания внутрь предметов или их макетов. Замену предметов, обработанных порошкообразным СХВ, следует производить в зависимости от местных климатических условий, но не реже одного раза в год, при герметизации смеси, и одного раза в квартал — при отсутствии герметизации, т. к. порошки СХВ легко впитывают влагу из воздуха, что ухудшает их свойства.

Специальные мази представляют собой жировую основу, в которую вводятся красящие, люминесцирующие вещества или их смеси. В качестве основы используются вакуумная смазка, вазелин, солидол, конталин и др. При приготовлении спецмази необходимо учитывать свойства жировой основы. Так, мазь на основе вазелина можно использовать в интервале температур от –3 °С (при дальнейшем понижении температуры она затвердевает) до +25 °С (при дальнейшем повышении температуры мазь легко разжижается).

Спецмази на основе конталина и вакуумной смазки более устойчивы к колебаниям температуры и влажности. Спецмазь на основе вакуумной смазки обладает большой липкостью и ограниченной растворимостью. Даже после удаления ее бензином следы люминесцирующих веществ могут быть обнаружены по характерному свечению в ультрафиолетовых лучах.

Хорошо зарекомендовала себя спецмазь, приготовленная на основе вакуумной смазки и вазелинового масла (в весовым отношении 3 : 1). Она удерживается на любых гладких поверхностях, не меняет своей консистенции в интервале температур от –20 °С до +30 °С.

Специальные мази наносят на предметы или их упаковки. В отличие от порошкообразных СХВ они хорошо удерживаются на различных гладких поверхностях. Следует также учитывать, что жировая основа изолирует СХВ от контактов

с влагой воздуха. Это обеспечивает сохранность пометок более длительное время даже в условиях повышенной влажности. Таким образом, если замену предметов, обработанных порошкообразным СХВ без герметизации, следует производить не реже одного раза в квартал, то при нанесении спецмази — не реже одного раза в год. Запаховые вещества, приготовленные в виде мази, легко впитываются шерстяными, хлопчатобумажными и другими тканями, хорошо удерживаются на различных поверхностях (дереве, металле, пластмассе, бетоне, резине, коже, грунтовых и асфальтированных дорогах). К тому же хорошо сохраняют красящие и люминесцирующие добавки от прямого воздействия внешних факторов, например, влажности и температуры.

Нанесение спецмазей производится при помощи кисти или ватного тампона.

Растворы СХВ приготавливаются на основе люминесцирующих веществ или индикаторов и применяются для пометки различных объектов. При приготовлении растворов может быть использована вода либо органические растворители, например, спирт, эфир, толуол, дихлорэтан, ацетон. При необходимости СХВ могут вводиться непосредственно в жидкости, которые необходимо пометить. Например, добавив в обычные синие или фиолетовые чернила люминесцирующие вещества, можно получить так называемые спецчернила. Их можно применять для нанесения перьевой ручкой меток на различные документы. При необходимости получить раствор, хорошо закрепляющийся на поверхности какого-либо объекта, в качестве растворителя может быть использован дихлорэтан, в который вводятся стружки оргстекла для образования трудносмываемой при высыхании пленки. Растворы СХВ наносятся на объекты с помощью кисточки, ручки, пульверизатора.

Специальные люминесцирующие карандаши используются для нанесения меток на различные объекты, документы, денежные знаки. Внешне ничем не отличаясь от обычных, эти карандаши имеют в составе своей стержневой массы специальную добавку — люминесцирующее вещество. Карандаши выпускаются нескольких цветов.

Перед нанесением меток необходимо убедиться, что помечаемые объекты сами не люминесцируют в ультрафиолетовых лучах. Цвет карандаша подбирается по цвету поверхности объекта. При нанесении меток на тонкие листы бумаги, документы, бумажную упаковку товаров необходимо следить, чтобы на них не оставалось вдавленных следов. В этих случаях под помечаемые объекты следует подкладывать предмет с твердой гладкой поверхностью, например, стекло или оргстекло.

Метки, нанесенные специальными люминесцирующими карандашами, сохраняются в течение длительного времени.

Аэрозольные распылители представляют собой баллон, наполненный смесью раствора люминесцирующего вещества или индикатора с фреонами. Когда применяют распылитель, из баллона под давлением паров фреона выбрасывается струя смеси и, дробясь на мельчайшие капли, образует аэрозольное облако.

Используя аэрозольные распылители, можно быстро и качественно обработать большие поверхности предметов, затратив небольшое количество СХВ. На вооружении в ОВД имеются следующие люминесцирующие аэрозоли: «Мадизол-М», «Мадизол-ПП», «Мадизол-СЖ».

«Мадизол-ПП» используется для пометки пищевых продуктов.

«Мадизол-М» применяется для нанесения меток на меховые и шерстяные изделия, хлопчато-бумажные и синтетические ткани.

«Мадизол-СЖ» предназначен для пометки строительных материалов, кожи, стекла, керамики, пластмассы, шерстяного покрова сельскохозяйственных животных.

На основе фенолфталеина выпускается ***«Фенозоль»***. Аэрозольная упаковка «Фенозоль» может иметь дозирующий клапан. Фенозоль используется для пометки спиртосодержащих жидкостей. Наличие фенозоля выявляется с помощью щелочного раствора.

Таким образом, в ОВД имеется на вооружении достаточное количество специальных химических веществ, которые могут быть эффективно применены в борьбе с преступностью. Однако это дает положительный результат лишь в том случае, если их следы будут быстро обнаружены в ходе проведения оперативно-розыскных действий.

§ 3. Понятие и виды химических ловушек

Проблема мелких хищений существует с давних времен и, наверное, будет существовать всегда, поскольку повышение своего материального состояния легкодоступным способом в большей или меньшей степени характерно для каждого человека. Сегодня технические средства охраны, наблюдения и сигнализации обладают колоссальными возможностями, однако они не могут защитить личное имущество граждан от посягательства со стороны нечестных людей. Так как нельзя создать общество с сетью тотального видеоконтроля и наблюдения, используются другие методы решения проблемы.

Одним из методов, способствующих предотвращению и быстрому раскрытию имущественных преступлений, является применение различных химических и технических средств. К ним относятся специальные химические составы, которые на практике и в литературе часто называют химическими ловушками либо средствами-маркерами (некоторые ученые предлагают термин «криминалистические маркеры»). Такие вещества, попадая на одежду или тело преступника, оставляют трудно устранимые и хорошо заметные следы, что позволяет установить его незаконное проникновение в помещение, контакты с определенными предметами, источниками похищенных материалов и каналами их сбыта, дачу взятки и т. д. Применение специальных средств в борьбе с преступлениями предусмотрено законом о полиции (п. 9 ст. 11), в котором они именуются «специальными окрашивающими средствами».

В Приказе Министерства внутренних дел Российской Федерации (МВД РФ) от 11.09.1993 № 423 дается следующая трактовка понятия химической ловушки: *это снаряженные (обработанные) специальными химическими веществами (красящие или запаховые) приспособления или устройства, закамуфлированные под различные предметы, с помощью которых такие вещества переносятся на тело и одежду человека.*

Химические ловушки — одно из средств раскрытия преступлений. Они отвечают всем требованиям, предъявляемым к техническим средствам, а следовательно, являются законными и их применение не должно вызывать сомнения. Идея создания ловушек подсказана самой практикой. Сотрудникам уголовного розыска хорошо известны факты, когда раскрытие краж значительно облегчалось, если преступник в момент совершения преступления случайно пачкал свои руки, обувь или одежду масляной краской, побелкой или другими красящими веществами. Подобные факты рассматривались как большая удача, так как это демаскировало преступника среди окружающих и способствовало быстрому его задержанию. Разработка и использование химических ловушек превращает удачи в закономерность,

поскольку препараты ловушек при попадании на тело человека и его одежду вызывают появление ярко окрашенных и трудно смываемых следов, легко бросающихся в глаза окружающим, что способствует задержанию преступника. Химические ловушки следователи самостоятельно не применяют, но они часто с ними встречаются при расследовании взяточничества, а также краж из торговых точек, подсобных и складских помещений, аптек, из служебных столов в учреждениях. Вещества выбрасывались устройствами на нарушителя при попытке несанкционированно вскрыть или взять снаряженный предмет. При этом происходило обильное окрашивание, а специфическое свойство красителя — проникать в поры тела или структуру одежды и обуви — позволяло распознать нарушителя в течение очень длительного времени. Даже если видимые следы красителя смылись, они очень ярко проявлялись в ультрафиолетовых лучах.

Состав используемых веществ включает базовые смеси с добавками. Они снаряжаются красителями нескольких цветов или их комбинацией, что позволяет использовать их для пометки товара определенного вида или конкретной территории. В случае задержания человека, вступившего в контакт с химической ловушкой, можно безошибочно установить его причастность к конкретному преступлению, даже если похититель будет умалчивать о ней или вообще отрицать. Нередко с помощью ловушек похитителя можно выявить раньше, чем будет обнаружено само хищение.

Химические ловушки, работая автономно, не требуют электропитания и дополнительного оборудования при установке и эксплуатации, а в комплексе с охранной сигнализацией дают еще больший эффект, особенно когда похититель совершает кражу «рывком».

Наряду с оказанием помощи по охране материальных ценностей на торговых объектах, базах, складах и в подсобных помещениях часто возникает необходимость в защите личной собственности конкретного человека. При высоком техническом уровне современной жизни очень мало средств используется для профилактики, документирования и раскрытия по горячим следам уже совершенных краж личного имущества, которые нередко совершают друг у друга сидящие рядом сотрудники. Причина заключается не в том, что нет подобных средств, — просто вступает в силу принцип рациональности и целесообразности из-за их высокой стоимости. При этом отодвигается на второй план как психологическая травма, так и материальный ущерб пострадавшего. Химические ловушки действуют исключительно «на вора» или «любопытного» сотрудника.

В связи с тем, что хищений личной собственности существует великое множество, химические ловушки изготавливаются конструктивно приближенными к предметам, представляющим интерес для похитителя. Используются материалы и прикрытия, которые находятся в месте установки химической ловушки: в обменных пунктах, банках и их филиалах, почтовых отделениях применяются банковские пакеты с соответствующими надписями, в магазинах и киосках — специальные шкатулки, способные создать иллюзию, что в них находятся деньги, на рабочих местах — кошельки и сумочки и т. д.

Разработчики и изготовители химических ловушек стараются выполнять запросы и пожелания заказчиков. Из-за возросшего количества краж из дач и погребов успешно применяется устройство отпугивания вора с помощью слезоточивого газа. Проникнув в строение и перемещаясь по нему, вор непременно зацепит тонкую капроновую леску, которая через пружинный механизм открывает клапан контейнера со слезоточивым газом. Даже если помещение большое, находиться в нем станет не-

возможно. Это устройство работает практически в любых климатических условиях, полностью энергонезависимо, не требует технического обслуживания, но устанавливать его необходимо в закрытых, маловентилируемых помещениях.

В связи с массовым распространением в последнее время такого вида преступлений, как хищение цветных металлов в промышленной аппаратуре, прошла успешное испытание химическая ловушка с пружинным механизмом выброса красителя. Принцип ее действия заключается в работке пружинного механизма при несанкционированном открытии или снятии оборудования. При этом на нарушителя выбрасывается порция красящего вещества. Ловушка сохраняет рабочие свойства на протяжении нескольких лет даже в экстремальных климатических условиях эксплуатации, что является первым требованием к таким устройствам. Она используется с целью предотвращения, а в случае совершения кражи из заблокированного объекта — быстрейшего раскрытия хищения.

Ловушка с пружинным механизмом выброса красителя устанавливается в электрощитовых шкафах и боксах связи, ящиках пожарных гидрантов и особенно пригодна для защиты таксофонного оборудования — телефонных будок с алюминиевой обшивкой и новых таксофонов, которые часто подвергаются нападению со стороны «охотников» за цветными металлами. В процессе изготовления учтены все проблемные вопросы, которые возникают при эксплуатации подобных устройств.

Как показала практика, после срабатывания химической ловушки — независимо от того, раскрыт ли похититель, — информация о факте применения подобных устройств надолго уничтожает стремление к воровству.

Химические ловушки по предназначению подразделяются на две группы:

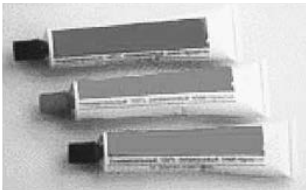
1) для нанесения меток;

2) для блокировки объектов с материальными ценностями.

Для нанесения меток на деньгах, ценных бумагах, различных предметах (например, передаваемых в качестве взятки) в настоящее время выпускаются следующие ловушки:

1. ***Комплект реактивов и приспособлений «Рододендрон»*** — предназначен для нанесения меток на денежные купюры.

2. ***Специальное средство в аэрозольной упаковке «Светлячок»*** — предназначено для нанесения на денежные знаки, документы и другие объекты тонкого слоя люминесцентного вещества, обладающего повышенной адгезией (в пер. с лат. — прилипание) к кожному покрову человека и невидимого в обычных условиях. При контакте пальцев рук, на которых имеется препарат, с различными поверхностями (дверной ручкой и т. п.) остаются следы пальцев, видимые под действием ультрафиолетового излучения с длиной волны 365 нм. Площадь поверхности, обрабатываемой из одной аэрозольной упаковки, — 1,5 м^2. Для этих целей применяется также красящая композиция «Помадка», изготовленная путем смешивания специальных красителей с определенными видами смазок. При контакте с ней на руках и одежде остаются трудно смываемые, маслянистые пятна малинового цвета.



3. ***Специальное средство «Диско»*** представляет собой косметический роллер, в который заправлен прозрачный гель со специальным люминесцентным маркером, невидимым при обычном освещении, позволяющий подтвердить легитим-

ность посетителя общественных мероприятий без предъявления пропуска. Соответствующая невидимая метка наносится контролером на руку посетителя путем прокатки шарика дозатора. Присутствие маркера может быть обнаружено по синему люминесцентному свечению при облучении ультрафиолетом с длиной волны 365 нм.

4. ***Маркирующие фломастеры «М»*** и ***«К»*** предназначены для нанесения меток, надписей на различные предметы и документы с целью их идентификации или исключения подделки. Фломастеры марки «М» используются для нанесения меток на бумажные материалы, марки «К» — для нанесения меток на предметы из металлов, пластмасс, кожи, тканей и т. п. В ультрафиолетовых лучах фломастеры «М» дают голубое свечение, «К» — зеленое.

5. ***Люминесцентные маркеры в виде восковых карандашей (мелков)*** предназначены для нанесения меток, невидимых при обычном освещении. Ими помечаются различные предметы — упаковочные коробки, ящики и т. п. Проверка подлинности и сохранности упаковки осуществляется при освещении ультрафиолетом с длиной волны 365 нм по характерному разноцветному свечению. Полный комплект состоит из 5 мелков различного свечения: желтого, зеленого, желто-зеленого, синего и красного.

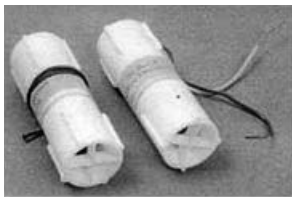
6. ***Люминесцентный маркер «Лак-М»*** предназначен для защиты различных предметов с целью выявления фактов подмены или несанкционированного вскрытия. Метка наносится на чистую твердую поверхность. Материалы, пригодные для ее нанесения — искусственная и натуральная кожа, металлы, пластмассы, дерево и т. п. О подлинности предмета судят по характерному желто-зеленому свечению метки в ультрафиолетовых лучах, возникающему после высыхания растворителя.

Химические ловушки, предназначенные для блокировки объектов с материальными ценностями, подразделяются на активные и пассивные.

Активные химические ловушки имеют устройство для выбрасывания красящего вещества в пространство и таким образом обеспечивают его попадание на одежду и открытые части тела человека, приведшего в действие это устройство. Выброс красителя может производиться как при срабатывании механических устройств, например пружинного, так и при срабатывании пиротехнического распылителя. В качестве пиротехнических распылителей в ловушках разрешается использовать только централизованно поставляемые специальные изделия (пиропатроны). Перед выходным отверстием таких изделий устанавливается щиток, не позволяющий осуществить прямой выброс химического вещества в лицо.

В последнее время стали выпускаться ***жидкостные маркеры «Купель».*** При несанкционированном вскрытии объекта происходит замыкание контакта и производится моментальный выброс распыленного красителя, сохраняющего ярко-крас-

ный цвет в течение 3 сут, а также люминесценцию в ультрафиолетовых лучах. Дальность выброса красителя составляет не менее 1,5 м, объем красителя — 1,5 мл. Маркер может использоваться в специальном изделии «Керн». Последнее имеет устройство для подключения к нему двух изделий «Купель». Срабатывание происходит от сигнала магнитного датчика либо посредством механического контакта. Площадь рассеивания — 5 м^2.



Химическая ловушка «Кукла-МГ» выполнена в виде денежных пачек объемом 100 листов. При ее изъятии с места происшествия производятся выброс красящей композиции и распыление слезоточивого состава.

Ловушка «Кошелек» имеет вид бумажника. При его вскрытии происходит распыление красящего вещества и включается сирена мощностью 80 дБ, а ***ловушка «Кредит»*** изготовляется в виде денежной упаковки из десяти пачек. При ограблении изделие передается грабителям вместе с настоящими деньгами, и через 5 мин с момента передачи происходят распыление слезоточивой композиции и интенсивное выделение дыма оранжевого цвета, что сильно затрудняет преступникам возможность бегства.

Для дистанционного маркирования различных материальных объектов и правонарушителей производится ***средство «Капрал».*** В его комплект входят две капсулы с красящим веществом, пять пиротехнических капсул со слезоточивым веществом и электрический фонарь для подсветки документов в темное время суток.

Пассивные химические ловушки срабатывающих устройств не имеют. Их конструкция рассчитана на непосредственное контактирование с ними лица, совершающего преступление. В таких ловушках красящее вещество в виде порошкообразных смесей или мазей либо наносится непосредственно на предмет, который может привлечь внимание преступника, либо помещается в пакеты, парафиновые капсулы или другую упаковку и маскируется среди подобных предметов.

Пассивные ловушки камуфлируются в упаковке винно-водочных изделий, кобурах огнестрельного оружия, банковских упаковках, дамских и инкассаторских сумках, трубках телефонов-автоматов, коробках для различных сувениров и дорогих конфет, оберток для плиток шоколада, в коробках для наркотических средств и т. п. При вскрытии таких объектов краситель просыпается и красящее вещество попадает на тело и одежду злоумышленника. Нередко на базе вазелина и красящих веществ приготавливаются мази, которыми обрабатываются специальные коврики. Они по окончании рабочего дня укладываются у дверей, на подоконниках. В случае проникновения преступника через двери или окна его обувь окрашивается в яркий цвет и можно проследить его маршрут движения с места происшествия, а затем использовать и как доказательство по делу.

Препарат «Б-1» — маркер в виде порошка, представляющий собой тонкодисперсное порошкообразное люминесцентное вещество с повышенной адгезией к кожному покрову человека. Предназначен для выявления фактов несанкционированного доступа, а также случаев хищения и взяточничества.

Препарат «Б-2» — маркер в виде мази; представляет собой суспензию с повышенной адгезией к кожному покрову человека. Предназначен для выявления фактов несанкционированного доступа, а также случаев хищения. Может наноситься на поверхность предметов, состояние и местонахождение которых необходимо определить или проследить. При соприкосновении с такими предметами на руках злоумышленника остается некоторое количество препарата.

В централизованном порядке используется ***изделие «Ковер».*** Оно состоит из тканевой подложки с приклеенными к нему микрокапсулами с запаховым веществом СП-80 МС. При воздействии на капсулы ноги человека они разрушаются, препарат попадает на подошву обуви, что значительно повышает работоспособность служебно-розыскных собак.

Срабатывание активных химических ловушек сопровождается определенным шумом (выстрел пиропатрона, щелчок пружины) и всегда является очевидным для преступника. В отличие от них факт действия пассивной ловушки преступник может обнаружить только через некоторое время.

Один и тот же объект может быть заблокирован как активными, так и пассивными химическим ловушками. При этом нередко наряду с химическими ловушками устанавливаются предметы, облегчающие оставление следов пальцев преступника.

К химическим ловушкам предъявляются следующие требования:

1. Ловушки должны быть безопасными для человека. На вооружение берутся лишь такие средства, в которых используются безвредные для человека химические вещества, а сила их выбрасывания не может вызывать механических повреждений глаз или иных органов. Например, при разработке пиропатрона, предназначенного для выбрасывания химического красителя, с особой тщательностью определялась навеска взрывчатого вещества. Патрон был взят на вооружение только после медико-биологических испытаний на кроликах и других живых организмах и получения по их результатам медицинского заключения.

2. Конструкция химических ловушек должна постоянно изменяться. Как отмечалось выше, о фактах использования таких маркеров для блокировки объектов с материальными ценностями известно многим лицам, склонным к совершению преступлений. При применении ловушек одних и тех же конструкций преступники быстро научатся их распознавать и при совершении краж не будут их касаться. Использование разнотипных средств позволяет избежать этого. К тому же многообразие конструкций ловушек необходимо и в связи с тем, что приходится блокировать самые разнообразные объекты (магазины, аптеки, раздевалки и пр.).

3. Химические ловушки должны быть надежными в эксплуатации, рассчитанными на длительное использование в различных климатических зонах. Применяемые в них красящие вещества, как правило, гигроскопичны, легко впитывают влагу. В условиях влажного климата, если не принять специальных мер по их защите от увлажнения, они могут быстро прийти в негодность, поэтому красящие вещества в следообразующих устройствах герметизируются (заделываются в плотные бумажные пакеты или помещаются в парафиновые капсулы).

4. В конструктивном отношении ловушки должны быть простыми, рассчитанными на использование подручных материалов и неквалифицированной рабочей

силы для их изготовления (курсантов полицейских школ и др.). В заводских условиях производятся только выбрасывающие устройства — пиропатроны, механические приспособления, базовые смеси красящих веществ. Они являются основой для любой конструкции, разрабатываемой непосредственно перед установкой. Это обеспечивает огромное разнообразие химических ловушек, что не позволяет преступникам их распознавать при совершении преступлений.

5. Химические ловушки должны быть дешевыми. Данное требование выдвигается в связи с тем, что такими средствами блокируется огромное количество объектов и если они будут дорогими, то для их изготовления потребуются значительные средства.

§ 4. Порядок применения химических ловушек

Выявление объектов хранения товарно-материальных ценностей, наиболее подверженных преступным посягательствам, и определение очередности их блокирования химическими ловушками осуществляют участковые инспектора полиции на основании анализа обстоятельств краж материальных ценностей и денежных средств, с учетом складывающейся оперативной обстановки. Это определено в Инструкции о порядке применения химических ловушек в раскрытии краж имущества, находящегося в государственной, муниципальной, частной собственности и собственности общественных объединений (организаций), утвержденной Приказом МВД РФ от 11 сентября 1993 г. № 423, введенной в действие 15 октября 1993 г. (далее — Инструкция) (прил. 1). При этом, как следует из Инструкции, выявление и блокирование указанных объектов — скорее правило для правоохранительных органов (их прямая обязанность), чем исключение, сделанное для назойливого собственника после его многочисленных обращений в различные инстанции. В любом случае блокирование объектов осуществляется с согласия собственника или уполномоченного им лица.

Перед блокировкой объекта химическими ловушками участковый полицейский в присутствии материально ответственных лиц проводит его обследование, чтобы установить количество, вид, камуфляж ловушек, места их установки. Количество ловушек и порядок их размещения внутри объекта определяются таким образом, чтобы создать максимальную вероятность вступления преступника в контакт с ними. Лица, материально ответственные за состояние блокируемого объекта, инструктируются о порядке обращения с установленными химическими ловушками.

Совместно с сотрудниками экспертно-криминалистических подразделений разрабатывается конструкция химических ловушек, организуется их изготовление. Состав красящего вещества определяет специалист-химик на основе поставляемых базовых смесей применительно к отдельной территориальной зоне. Последнее имеет большое значение, поскольку при задержании подозреваемого по обнаруженному на нем веществу можно установить район, где было совершено преступление.

По факту установления на объекте таких ловушек работник уголовного розыска или участковый инспектор оформляет акт (прил. 2) и карточку (прил. 3) определенной формы. В акте указываются наименование заблокированного объекта, должность и фамилия сотрудника полиции, установившего средство-маркер, фамилия, имя, отчество материально ответственного лица, внешний вид ловушки и описа-

ние используемого в ней химического вещества (без точного его наименования). Материально ответственное лицо подробно инструктируется о правилах обращения с ловушкой определенного вида и предупреждается о неразглашении факта ее установки. К акту приобщается в опечатанном виде пакетик с образцом красящего вещества. Список всех заблокированных данными средствами объектов хранится в дежурной части ОВД и используется для информирования следственно-оперативной группы, выезжающей на место происшествия при получении сообщения о совершении кражи. Факт срабатывания химических ловушек отражается в протоколе осмотра места происшествия, об этом по рации дается срочная информация оперативным нарядам для розыска преступника по горячим следам. К протоколу приобщается образец красящего вещества, если в результате срабатывания ловушки оно частично просыпалось.

Нередко химическую ловушку (часто пассивную) преступники уносят с собой. В таких случаях следователь в протоколе осмотра указывает, что со слов материально ответственного лица, участвующего в осмотре, в таком-то месте накануне кражи находилась химическая ловушка, которая в момент осмотра не обнаружена. Более подробно этот факт фиксируется в протоколе допроса материально ответственного лица. Акт о блокировке объекта химической ловушкой и приложенный к нему образец красящего вещества затребуются из органа полиции и приобщаются к уголовному делу.

В случае выявления подозреваемого проводятся немедленное его освидетельствование и осмотр одежды, личный обыск, обыск по месту жительства и работы. Во всех случаях используется ультрафиолетовый осветитель. При обнаружении на теле вещества, которое могло образоваться веществом химической ловушки, оно изымается с помощью марлевого тампона, а одежда со следами такого вещества упаковывается и направляется на физико-химическую экспертизу. Производство экспертизы целесообразно поручать экспертно-криминалистическим подразделения МВД, УВД, поскольку эксперты имеют информацию о зоне применения специального состава и владеют методикой исследования веществ, применяемых в химических ловушках.

Перед экспертизой обычно ставится два вопроса:

1) каков состав вещества, которым образовано пятно на одежде (теле) подозреваемого;

2) совпадает ли он с составом вещества химической ловушки, установленной на объекте, из которого совершена кража.

§ 5. Правовые аспекты применения химических ловушек

Единственным на сегодняшний день нормативно-правовым документом, регламентирующим порядок применения химических ловушек, является вышеупомянутая Инструкция о порядке применения химических ловушек в раскрытии краж имущества, находящегося в государственной, муниципальной, частной собственности и собственности общественных объединений (организаций), утвержденная Приказом МВД РФ от 11 сентября 1993 г. № 423, введенной в действие 15 октября 1993 года. Она представляет собой руководство в первую очередь для сотрудников правоохранительных органов, а не для потенциальных потребителей. Поэтому при трактовке ее положений необходимо учитывать, что нормами прямого действия они не являются.

Изготовлением химических ловушек занимаются технические отделы МВД, ГУВД, УВД. Поставка необходимого количества и ассортимента ловушек производится органами материально-технического снабжения указанных органов по заявлениям участковых инспекторов полиции. Таким образом, лица, заинтересованные в установке ловушек, могут обратиться с соответствующим запросом в местное отделение полиции. Вместе с тем существуют различные коммерческие фирмы, практикующие изготовление и установку химических ловушек, поскольку достаточной нормативной базы, позволяющей отнести этот сектор к исключительному ведению государственных органов, нет.

Так, Федеральный закон от 08 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности» в качестве деятельности, сопряженной с изготовлением химических ловушек, на осуществление которой необходима лицензия, называет лишь производство пиротехнических изделий. Указом Президента РФ от 22 февраля 1992 г. № 179 (в редакции от 30 декабря 2000 г.) утвержден перечень видов продукции (работ, услуг) и отходов производства, свободная реализация которых запрещена. Работы по изготовлению химических ловушек и услуги по их установке в данном перечне не значатся. Не запрещен их оборот и Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Ответственность за кустарное производство и распространение химических ловушек ни Кодексом об административных правонарушениях РФ, ни Уголовным кодексом РФ прямо не предусмотрена. В Инструкции о порядке применения химических ловушек также не сказано о том, что в задачи правоохранительных органов входит выявление объектов, блокированных с нарушением установленных Инструкцией правил, и изъятие контрафактных ловушек.

В любом случае при возникновении каких-либо бюрократических сложностей на стадии возбуждения дела, связанных с самовольной установкой ловушек и их несогласованным использованием, необходимо помнить, что уголовное дело или дело об административном правонарушении возбуждается по факту совершения противоправного действия или проступка, а не по факту срабатывания ловушки.

Однако несоответствие ловушек критериям качества, которые декларирует производитель или которые были заранее оговорены с заказчиком, может повлечь последствия для их производителя (распространителя) в виде ответственности, в том числе за невыполнение обязательств и нарушение прав потребителя. Ответственность указанных лиц может также наступать в случаях:

1) если ловушка сработала в неподходящий момент и в зоне распыления вещества оказался не злоумышленник;

2) если действием ловушки был причинен вред здоровью.

Проблема причинения вреда правам и интересам личности является немаловажной в вопросах использования химических ловушек. Если не брать в расчет случаи, когда посредством некачественной химической ловушки причиняется ущерб физическому состоянию человека, а рассматривать нарушения иных личных неимущественных прав, то ответ на данный вопрос заключается в способе действия красящего вещества, содержащегося в химических ловушках. В большинстве своем принцип действия прост: попадая на кожу злоумышленника, вещество не смывается в течение нескольких дней. Поэтому, если на месте совершения хищения выявлена поврежденная (сработавшая) ловушка и очевидно, что произошел выброс красящего вещества, подозрение в совершении хищения может пасть на любого сотрудника, который после происшествия не вышел на работу. Практике известны

случаи, когда сотрудники правоохранительных органов приходили к лицам, не вышедшим на работу якобы по причине недомогания, осведомиться о случившейся недавно в организации краже и заставали их со следами действия химических ловушек на лице или руках.

Иногда химическому веществу придают такие свойства, благодаря которым оно не оставляет ярких пятен, а становится заметным лишь при попадании на него ультрафиолетовых лучей. Правонарушитель может этого не знать и соответственно не принять мер предосторожности при появлении в обществе других людей. Такие ловушки наиболее действенны. Вместе с тем их применение может повлечь нарушение личных неимущественных прав граждан, в частности чести, достоинства и репутации. Ведь если сотрудник, одежда или кожа которого испачканы химическим веществом, «засветится» в кругу коллег, его доброе имя пострадает, как минимум, в рамках данной организации, даже если он впоследствии будет признан невиновным. В определенных условиях использование таких ловушек может быть расценено как средство получения информации о личности без ее ведома и согласия, что является нарушением положений Конституции РФ, Федерального закона от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации, защите информации» и ряда других нормативных актов.

Так, в соответствии со ст. 86 Трудового кодекса РФ «все персональные данные (информацию о личности) работника следует получать у него самого. Если такие данные возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение».

Данный подход согласуется и с процессуальным законодательством, в частности с положениями о законности получения доказательств. Поэтому к использованию ловушек скрытого действия следует подходить особенно осторожно. Сохранить тайну следствия отчасти могут помочь заранее проработанные аргументы, например объяснение трудовому коллективу о случайной порче (повреждении оболочки) химической ловушки, проведении учений или некоего эксперимента, не связанного с участившимися случаями хищения на складе.

Вместе с тем сообщение сотрудникам складов, производственных баз и иных мест сосредоточения товарно-материальных ценностей о том, что объект, на котором они работают, оборудован химическими ловушками, может послужить гарантом сохранности казенного имущества.

Информирование может производиться не только путем прямого объявления об этом на собрании коллектива, но и, например, путем включения в типовую форму трудового договора (контракта) соответствующего пункта: «Работник информирован о том, что работодатель, в целях предотвращения хищений и других посягательств на принадлежащее ему имущество, намерен использовать различные охранные технические и химические средства, в том числе оборудовать места сосредоточения товарно-материальных ценностей химическими ловушками. Работник не возражает против использования работодателем указанных средств».

ИНСТРУКЦИЯ
о порядке применения химических ловушек в раскрытии краж имущества, находящегося в государственной, муниципальной, частной собственности и собственности общественных объединений (организаций)

1. Химические ловушки*— это снаряженные (обработанные) специальными химическими веществами (красящие или запаховые) приспособления или устройства, закамуфлированные под различные предметы, с помощью которых такие вещества переносятся на тело и одежду человека.

2. Химические ловушки могут быть активного и пассивного типа.

В ловушках активного типа химические вещества переносятся на объект при срабатывании механического или пиротехнического распылителя. В качестве пиротехнических распылителей в ловушках разрешается использовать только централизованно поставляемые специальные изделия (пиропатроны). Перед выходным отверстием таких изделий необходимо ставить щиток, не позволяющий осуществлять прямой выброс химического вещества в лицо.

В ловушках пассивного типа контакт с химическим веществом происходит в момент нарушения оболочек ловушек или непосредственно при соприкосновении со специальными открытыми веществами (мазями).

Специальное химическое вещество в ловушках активного и пассивного типа надежно изолируется от воздействия внешней среды.

3. Блокировке ловушками подлежат объекты сосредоточения товарно-материальных ценностей (склады, базы, магазины, аптеки и другие помещения), а также места временного хранения денежных средств (сбербанки, кассы предприятий, учреждений, коллективных хозяйств и других организаций) с согласия собственника или уполномоченного им лица.

4. На основании анализа обстоятельств краж материальных ценностей, денежных средств и с учетом оперативной обстановки, складывающейся на обслуживаемой территории, участковые инспектора полиции выявляют объекты хранения товарно-материальных ценностей, наиболее подверженные преступным посягательствам, и определяют очередность их блокировки ловушками.

5. Перед блокировкой объектов участковый инспектор полиции проводит их обследование с целью определения количества, видов, камуфляжа ловушек (упаковки), мест их установки, с учетом особенностей хранящихся материальных ценностей, технической укрепленности объектов и других условий.

6. Количество и размещение ловушек внутри объектов хранения товарно-материальных ценностей определяются таким образом, чтобы обеспечивалась максимальная вероятность вступления в контакт с ними преступников. При проведении мероприятий службой криминальной полиции сотрудники оперативных подразделений могут установить комплекты ловушек для решения своих оперативно-тактических задач. Об установке ловушек они обязаны проинформировать участкового инспектора полиции, на территории обслуживания которого находится заблокированный объект.

7. Обследование и блокирование объектов ловушками проводится участковыми инспекторами полиции в присутствии материально ответственных лиц, которые инструктируются о порядке обращения с ловушками. Информация о заблокированных объектах на обслуживаемой территории заносится участковыми инспекторами полиции в соответствующий раздел паспорта на участок.

8. При установке ловушек участковыми инспекторами полиции составляется акт**, к которому в герметичной упаковке приобщается образец химического вещества. В случае применения способа заряжения ловушек нестандартным химическим веществом в техническом отделе к акту приобщается образец данного химического вещества в герметичной упаковке. При использовании одного химического вещества для нескольких ловушек разрешается иметь один опечатанный образец химического вещества с указанием в каждом акте номера печати и места установки. Кроме того, на каждый объект, где установлены ловушки, участковыми инспекторами составляется карточка, которая вместе с актами по установке ловушки и опечатанными образцами химических веществ хранится в сейфе дежурной части органа внутренних дел в картотеке. Допуск к картотеке разрешен участковым инспекторам и сотрудникам оперативных подразделений.

Контроль за ведением картотеки осуществляется одним из заместителей начальника горрайоргана внутренних дел. Один раз в квартал участковые инспектора проверяют состояние химических ловушек и в случае сомнения в их работоспособности производят замену на новые.

Снятые с объекта ловушки направляются в технические отделы для принятия решения о возможности их дальнейшего применения или снятия с учета.

9. Заявки на централизованное изготовление, поставку необходимого количества и ассортимента ловушек направляются в органы материально-технического снабжения или непосредственно в технические отделы МВД, ГУВД, УВД.

10. Если при осмотре места происшествия в случае кражи с объекта хранения товарно-материальных ценностей обнаружено нарушение целостности ловушек, в протоколе обязательно указывается факт обнаружения химических веществ.

11. В случае задержания подозреваемых в краже лиц к протоколу приобщаются одежда, предметы со следами химических веществ, а также смывы красителя с кожных покровов задержанного. Сравнительное исследование химических веществ, изъятых с кожных покровов и одежды подозреваемого лица, и образца химического вещества, установленного и нарушаемого на заблокированном объекте, производится экспертно-криминалистическими подразделениями.

12. Использование ловушек при проведении разовых оперативно-розыскных мероприятий осуществляется с разрешения начальника органа внутренних дел или его заместителя по криминальной полиции.

*Наименования химических ловушек

«Растяжка» (белый дым) — предназначена для охраны помещений. При обрыве нити (тонкой проволоки), натянутой на уровне 10 см над полом, срабатывает дымовой патрон и охраняемое помещение заполняется белым дымом (50 м^3), что дезориентирует преступника и заставляет его быстро покинуть помещение.

«Ювелирный футляр» — коробочка для ювелирных изделий, внутри которой находится капсула со специальным химическим веществом (СХВ). При открывании футляра происходит выброс СХВ, окрашивая руки, одежду и лицо злоумышленника в ярко-красный цвет.

«Бутылка» — емкость под винно-водочные изделия. Под металлической пробкой находится пластмассовая капсула с СХВ. При открывании бутылки происходит выброс СХВ.

«Коврик» (коврик и специальная мазь) — химическая ловушка напольного типа в виде коврика типа «травка» с нанесенной специальной родаминовой мазью.

Обычно располагается на ночь у входа в помещение. При наступании на коврик на подошве обуви преступника остается специальная мазь, окрашивающая подошву в красный цвет. Преступник оставляет характерные следы красного цвета.

«Коробка» — химическая ловушка с электропиротехническим устройством «Купель», которое вмонтировано в различные виды коробок. При вскрытии коробки замыкается электрическая цепь и происходит выброс СХВ.

«Керн» — унифицированная многоразовая химическая ловушка активного типа. Предназначена для распыления СХВ посредством установленных в корпусе двух электропиротехнических устройств «Купель». Изделие срабатывает от включения герконового переключателя при удалении магнитного элемента от корпуса изделия или от срабатывания механического переключателя. Устанавливается в сейфах и шкафах.

«Сотовый телефон» — сотовый телефон типа «раскладушка» (аналог моделей «Samsung SGH X460», «Nokia 6101» и т. д). Для того чтобы воспользоваться телефоном данного типа, его необходимо раскрыть. При раскрывании телефона замыкается контактная группа и происходит выброс СХВ-порошка «родамин», окрашивающего руки и одежду злоумышленника в ярко-красный цвет.

«Утренняя звезда» — люминесцентные бесцветные чернила.

«СФ» — бесцветный фломастер для нанесения люминесцентных меток.

«Черная звезда» — специальные черные чернила со свечением на оттиске.

ЧСР1, ЧСР2 («рододендрон») — реактивные чернила. Метка не видна при обычном и УФ-освещении. При обработке проявителем возникает изображение синего или красного цвета.

«ФШК» — штемпельная краска люминесцирующая (цвет краски и свечение люминесцентной добавки определяются по согласованию).

«ФШК-Б» — штемпельная бесцветная люминесцирующая краска (цвет люминесценции: синий, красный, желтый, зеленый).

«ЛЮМО» — люминесцентный маркер для нанесения на твердые поверхности.

«Фломастер-М», «Фломастер-К» — люминесцентные маркеры повышенной стойкости для твердых поверхностей.

«Лак-М» — люминесцентный маркер для гидрофобных поверхностей.

Мелки УФ — мелки маркировочные люминесцирующие; в наборе зеленый, желтый, желто-зеленый, красный, бирюзовый цвета.

Мелки ТХ — мелки маркировочные термохромные, меняют цвет на розовый или бесцветный при нагреве до 50–65 оС.

«Василек» — люминесцентное средство защиты бумажной продукции от подмены и подделки.

«Диско» — люминесцентный маркер-роллер для кожи рук.

«Родамин», «Зеленка», «Лютик» — химические ловушки (трудно смываемый красящий состав в виде порошка или мази).

«Огонек» — люминесцентное метящее средство — паста с повышенной адгезией к коже рук.

«Орлюм» — люминесцентное метящее средство с повышенной адгезией к коже рук человека.

«Б-1» — люминесцентное метящее средство повышенной секретности и высокой адгезией к коже рук человека (порошок).

«Б-2» — люминесцентное метящее средство повышенной секретности и высокой адгезией к коже рук человека (мазь).

«Кукла» — изделие (муляж) с красящим составом.

«Кукла-МГ» — изделие (муляж) с красящим составом и слезоточивым газом.

«Кукла-МД» — изделие (муляж) с дымовым составом.

«Купель» — изделие с красящим составом (пиротехнический заряд срабатывает от источника электропитания).

«Катапульта» — изделие с красящим составом (пиротехнический заряд срабатывает от терочного механизма).

«Кошелек» — химическая ловушка в виде кошелька с выбросом краски.

«Кошелек-М» — химическая ловушка в виде кошелька с выбросом краски и звуковой сиреной.

«Барсетка» — химическая ловушка в виде барсетки с выбросом краски и звуковой сиреной.

«НОВО-ФЛ-1», «НОВО-ФЛ-2», «НОВО-ФЛ-3» — комплекты химических ловушек.

«НОВО-ФЛ-4» — комплект химических ловушек повышенной секретности.

****АКТ**
об установке химической ловушки

Дата Населенный пункт

Я, _____

_____
(Фамилия, имя, отчество, должность сотрудника)

в присутствии _____

_____
(Фамилия, имя, отчество, должность материально ответственного лица)

Установил _____

_____
(Наименование объекта, адрес)

химическую ловушку _____

_____
(Описываются внешний вид и непосредственное место установки химической ловушки)

Подпись: _____

С правилами обращения с ловушкой ознакомлен(а)

_____
(Подпись лица, ответственного за использование ловушки)

Тема 7. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

§ 1. Выявление каналов утечки и несанкционированного доступа к ресурсам

В настоящее время необходимость в защите информации, содержащейся в информационных системах правоохранительных органов, не вызывает сомнений. Сущность защитных мероприятий сводится к перекрытию возможных каналов утечки защищаемой информации, которые появляются в силу объективно складывающихся условий ее распространения и возникающей у конкурентов заинтересованности в ее получении. Каналы утечки информации достаточно многочисленны. Они могут быть как естественными, так и искусственными, т. е. созданными с помощью технических средств. Перекрытие всех возможных каналов несанкционированного съема информации требует значительных затрат, и, поэтому, в полном объеме сделать это удается далеко не всегда. Следовательно, в первую очередь необходимо обратить внимание на те из них, которыми с наибольшей вероятностью могут воспользоваться недобросовестные конкуренты. Наибольшую привлекательность для злоумышленников представляют акустические каналы утечки информации, в особенности такой канал, как виброакустический (за счет распространения звуковых колебаний в конструкции здания). Рассмотрим возможные каналы утечки информации и несанкционированного доступа к ресурсам, которые могут быть использованы противником в данном помещении, а также возможную защиту от них. В настоящее время номенклатура технических средств разведки весьма обширна, что делает задачу надежного блокирования каналов утечки и несанкционированного доступа к информации исключительно сложной (табл. 7.1.1). Решение подобной задачи возможно только с использованием профессиональных технических средств и с привлечением квалифицированных специалистов.

Таким образом, основным направлением противодействия утечке информации является обеспечение физической (технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность достигается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Основными причинами утечки информации являются:

- несоблюдение персоналом норм, требований, правил эксплуатации аппаратной среды (АС);
- ошибки в проектировании АС и систем защиты АС;
- ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации АС может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что в данном случае лицом, совершающим несанкционированные действия, двигают личные побудительные мотивы. Причины утечки информации достаточно тесно связаны с видами утечки информации.

Таблица 7.1.1 — Основные методы и средства несанкционированного получения информации и возможная защита от них

№ п/п	Действие человека (типовая ситуация)	Каналы утечки информации	Методы и средства получения информации	Методы и средства защиты информации
1	Разговор в помещении	• Акустика • Виброакустика • Гидроакустика • Акустоэлектроника	• Подслушивание, диктофон, микрофон, направленный микрофон, полуактивная система • Стетоскоп, вибродатчик • Гидроакустический датчик • Радиотехнические спецприемники	Шумовые генераторы, поиск закладок, защитные фильтры, ограничение доступа
2	Разговор по проводному телефону	• Акустика • Электросигнал в линии • Наводки	• Аналогично п. 1 • Параллельный телефон, прямое подключение, электромагнитный датчик, диктофон, телефонная закладка	• Аналогично п. 1 • Маскирование, скремблирование, шифрование • Спецтехника
3	Разговор по радиотелефону	• Акустика • Электромагнитные волны	• Аналогично п. 1 • Радиоприемные устройства	• Аналогично п. 1 • Аналогично п. 2
4	Документ на бумажном носителе	Наличие	Кража, визуально, копирование, фотографирование	Ограничение доступа, спецтехника
5	Изготовление документа на бумажном носителе	• Наличие • Паразитные сигналы, наводки	• Аналогично п. 4 • Специальные радиотехнические устройства	• Аналогично п. 1 • Экранирование
6	Почтовое отправление	Наличие	Кража, прочтение	Специальные методы защиты
7	Документ на небумажном носителе	Носитель	Хищение, копирование, считывание	Контроль доступа, физическая защита, криптозащита
8	Изготовление документа на небумажном носителе	• Изображение на дисплее • Паразитные сигналы, наводки	• Визуально, копирование, фотографирование • Специальные радиотехнические устройства	Контроль доступа, криптозащита
9	Передача документа по каналу связи	Электрические и оптические сигналы	Несанкционированное подключение, имитация зарегистрированного пользователя	Криптозащита
10	Производственный процесс	Отходы, излучения и т. п.	Спецаппаратура различного назначения, оперативные мероприятия	Оргтехмероприятия, физическая защита

В соответствии с ГОСТ Р 50922—96 рассматриваются три вида утечки информации:

- разглашение;
- несанкционированный доступ к информации;
- получение защищаемой информации разведками (как отечественными, так и иностранными).

Под разглашением информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Под несанкционированным доступом понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Получение защищаемой информации разведками может осуществляться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка).

Канал утечки информации — совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может располагаться в пределах контролируемой зоны, охватывающей аппаратную среду, или вне ее.

Применительно к АС выделяют следующие каналы утечки:

1. *Электромагнитный канал.* Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в аппаратных компонентах АС. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки). Электромагнитный канал в свою очередь делится на следующие каналы:

- радиоканал (высокочастотное излучение);
- низкочастотный канал;
- сетевой канал (наводки на сеть электропитания);
- канал заземления (наводки на провода заземления);
- линейный канал (наводки на линии связи между компьютерными системами).

2. *Акустический (виброакустический) канал.* Связан с распространением звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации АС.

3. *Визуальный канал.* Связан с возможностью визуального наблюдения злоумышленником за работой устройств отображения информации АС без проникновения в помещения, где расположены компоненты системы. В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т. п.

4. *Информационный канал.* Связан с доступом (непосредственным и телекоммуникационным) к элементам АС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также с подключением к линиям связи. Информационный канал может быть разделен на следующие каналы:

- канал коммутируемых линий связи,
- канал выделенных линий связи,
- канал локальной сети,
- канал машинных носителей информации,
- канал терминальных и периферийных устройств.

Возможные каналы утечки информации

Утечка акустической информации из-за применения подслушивающих устройств

Для перехвата и регистрации акустической информации существует огромный арсенал разнообразных средств разведки: микрофоны, электронные стетоскопы, радиомикрофоны или так называемые «радиозакладки», направленные и лазерные микрофоны, аппаратура магнитной записи. Набор средств акустической разведки, используемых для решения конкретной задачи, сильно зависит от возможности доступа агента в контролируемое помещение или к интересующим лицам.

Применение тех или иных средств акустического контроля зависит от условий применения, поставленной задачи, технических и, прежде всего, финансовых возможностей организаторов подслушивания.

Утечка информации за счет скрытного и дистанционного видеонаблюдения

Из средств данного типа наиболее широко применяются скрыто устанавливаемые фото-, кино- и видеокамеры с выходным отверстием объектива несколько миллиметров.

Используются также миниатюрные видеосистемы состоящие из микровидеокамеры с высокой чувствительностью и микрофоном. Устанавливаются на двери или в стене. Для конспиративного наблюдения используются также микровидеокамеры в настенных часах, в датчиках пожарной сигнализации, небольших радиомагнитолах, а также в галстуке или брючном ремне. Видеоизображение может записываться на малогабаритный видеомагнитофон или передаваться с помощью малогабаритного передатчика по радиоканалу в другое помещение или автомашину на специальный или стандартный телеприемник. Расстояние передачи, в зависимости от мощности передачи, достигает от 200 м до 1 км. При использовании ретрансляторов расстояние передачи может быть значительно увеличено.

Привлекает внимание автомобильная система скрытого видеонаблюдения. Видеокамера, обеспечивающая круговой обзор, закамуфлирована под наружную антенну сотового телефона. Плоский экран устанавливается либо на солнцезащитном козырьке, либо в «бардачке», пульт управления — или в пепельнице, или в кармане на двери. Видеосигнал, в зависимости от комплектации, может записываться прямо на видеомагнитофон либо передаваться по радиолинии на расстояние до 400 м. Видеокамера комплектуется сменными объективами с различными углами зрения.

Лазерный съем речевой информации

Для дистанционного перехвата информации (речи) из помещений иногда используют лазерные устройства. Из пункта наблюдения в направлении источника звука посылается зондирующий луч. Зондирующий луч обычно направляется на стекла окон, зеркала, другие отражатели. Все эти предметы под действием речевых сигналов циркулирующих в помещении колеблются и своими колебаниями модулируют лазерный луч, приняв который в пункте наблюдения, можно путем несложных преобразований восстановить все речевые сигналы, циркулирующие в контролируемом помещении. На сегодняшний день создано целое семейство лазерных средств акустической разведки. Такие устройства состоят из источника излучения (гелий-неоновый лазер), приемника этого излучения с блоком фильтрации шумов, двух пар головных

телефонов, аккумулятора питания и штатива. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Съем речевой информации с оконных рам с двойными стеклами с хорошим качеством обеспечивается с расстояния до 250 м. Такой возможностью, в частности, обладает система SIPE LASER 3-DA SUPER производства США.

Однако на качество принимаемой информации, кроме параметров системы, оказывают влияние следующие факторы:

- параметры атмосферы (рассеяние, поглощение, турбулентность, уровень фона);
- качество обработки зондируемой поверхности (шероховатости и неровности, обусловленные как технологическими причинами, так и воздействием среды — грязь, царапины и пр.);
- уровень фоновых акустических шумов;
- уровень перехваченного речевого сигнала.

Кроме того, применение подобных средств требует больших затрат не только на саму систему, но и на оборудование по обработке полученной информации. Применение такой сложной системы требует высокой квалификации и серьезной подготовки операторов.

Из всего этого можно сделать вывод, что применение лазерного съема речевой информации дорогое удовольствие и довольно сложное, поэтому надо оценить необходимость защиты информации от этого вида разведки.

Пути утечки информации в вычислительных системах

Вопросы безопасности обработки информации в компьютерных системах пока еще волнуют в нашей стране не слишком широкий круг специалистов.

До сих пор эта проблема более-менее серьезно вставала у нас, пожалуй, только перед рядом государственных и военных органов, а также перед научными кругами. Теперь же появилось большое число фирм и банков, эффективная деятельность которых практически немыслима без использования компьютеров. Как только должностные лица этих и других организаций это поймут, перед ними сразу же встанут именно вопросы защиты имеющейся у них критичной информации.

Так что, пока еще есть время, стоит очень серьезно задуматься над имеющимся зарубежным опытом, чтобы не изобретать собственного велосипеда. В частности, для начала небесполезно будет ознакомиться с классификацией и принципами оценивания безопасности компьютерных систем, используемыми в США. Различают два типа некорректного использования ЭВМ:

- доступ к ЭВМ лиц, не имеющих на это права;
- неправильные действия тех лиц, которые имеют право на доступ к ЭВМ (так называемый санкционированный доступ).

Обычно разработчиков систем волнует только решение второй проблемы. Анализ вероятных путей утечки информации или ее искажений показывает, что при отсутствии специальных мер защиты, обеспечивающих выполнение функций, возложенных на вычислительную систему, возможно:

- снятие дистанционными техническими средствами секретных сообщений с мониторов ЭВМ, с принтеров (перехват электромагнитных излучений);
- получение информации, обрабатываемой в ЭВМ, по цепям питания;
- акустическая или электроакустическая утечка вводимой информации;
- перехват сообщений в канале связи;
- навязывание ложного сообщения;
- считывание (изменение) информации ЭВМ при несанкционированном доступе;
- хищение носителей информации и производственных отходов;

- чтение остаточной информации в ЗУ системы после выполнения санкционированных запросов;
- копирование носителей информации;
- несанкционированное использование терминалов зарегистрированных пользователей;
- маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
- маскировка несанкционированных запросов под запросы операционной системы (мистификация);
- использование программных ловушек;
- получение защищаемых данных с помощью серии разрешенных запросов;
- использование недостатков языков программирования и операционных систем;
- преднамеренное включение в библиотеки программ специальных блоков типа «троянских коней»;
- злоумышленный вывод из строя механизмов защиты.

В особую группу следует выделить специальные закладки для съема информации с компьютеров.

Миниатюрный радиомаяк, встроенный в упаковку, позволяет проследить весь путь следования закупленной ЭВМ, транслируя сигналы на специальный передатчик. Узнав таким путем, где установлена машина, можно принимать любую обработанную компьютером информацию через специально вмонтированные электронные блоки, не относящиеся к ЭВМ, но участвующие в ее работе. Самая эффективная защита от этой закладки — экранированное помещение для вычислительного центра.

По мнению специалистов универсальных «компьютерных закладок» сегодня не бывает. Те закладки, которые удавалось обнаружить, можно условно разделить на три типа: те, которые выбирают информацию по ключевым словам или знакам, те, которые передают всю информацию, находящуюся на винчестере ЭВМ и просто уничтожающие ее.

Утечка информации за счет перехвата побочных электромагнитных излучений и наводок

Одной из наиболее вероятных угроз перехвата информации в системах обработки данных считается утечка за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами. ПЭМИН существуют в диапазоне частот от единиц Гц до полутора ГГц и способны переносить (распространять) сообщения, обрабатываемые в автоматизированных системах. Дальность распространения ПЭМИН исчисляется десятками, сотнями, а иногда и тысячами метров. Наиболее опасными источниками ПЭМИН являются дисплеи, проводные линии связи, накопители на магнитных дисках и буквопечатающие аппараты последовательного типа.

Например, с дисплеев можно снять информацию с помощью специальной аппаратуры на расстоянии до 500–1500 м, с принтеров — до 100–150 м. Перехват ПЭМИН может осуществляться и с помощью портативной аппаратуры. Такая аппаратура может представлять собой широкополосный автоматизированный супергетеродинный приемник. В качестве устройств регистрации принятых сигналов (сообщений) может использоваться магнитный носитель или дисплей.

Утечка информации при использовании средств связи и различных проводных коммуникаций

В данном случае, когда речь заходит о возможности перехвата информации при использовании линий связи и проводных коммуникаций, следует иметь в виду, что

перехват может осуществляться не только с телефонных линий и не только речевой информации. В этот раздел можно отнести:

- прослушивание и запись переговоров по телефонным линиям;
- использование телефонных линий для дистанционного съема аудио- информации из контролируемых помещений;
- перехват факсимильной информации;
- перехват разговоров по радиотелефонам и сотовой связи;
- использование сети 220 В и линий охранной сигнализации для передачи акустической информации из помещений;
- перехват пейджинговых сообщений.

Рассмотрим кратко каждый из перечисленных каналов утечки информации в отдельности.

Прослушивание и запись переговоров по телефонным линиям

Телефонные абонентские линии обычно состоят из трех участков: магистрального (от АТС до распределительного шкафа (РШ)), распределительного (от РШ до распределительной коробки (КРТ)), абонентской проводки (от КРТ до телефонного аппарата). Последние два участка — распределительный и абонентский являются наиболее уязвимыми с точки зрения перехвата информации. Подслушивающее устройство может быть установлено в любом месте, где есть доступ к телефонным проводам, телефонному аппарату, розетке или в любом месте линии вплоть до КРТ. Наиболее простой способ подслушивания это подключение параллельного телефонного аппарата или «монтерской» трубки. Используются также специальные адаптеры для подключения магнитофонов к телефонной линии. Адаптеры сделаны таким образом, что диктофон, установленный на запись в режиме акустопуска, включается только при поднятой трубке телефонного аппарата. Это дает возможность экономно расходовать пленку на кассете, не сматывая ее вхолостую.

Прослушивание телефонных линий может вестись не только гальванически (прямым подсоединением), а и с помощью индукционных или емкостных датчиков. Такое подсоединение практически не обнаруживается с помощью тех аппаратных средств, которые широко используются для поисковых целей.

Самыми распространенными из подобных средств прослушивания являются телефонные контроллеры радиоретрансляторы, которые чаще называются телефонными передатчиками или телефонными «закладками». Телефонные закладки подключаются параллельно или последовательно в любом месте телефонной линии и имеют значительный срок службы, так как питаются от телефонной сети. Эти изделия чрезвычайно популярны в промышленном шпионаже благодаря простоте и дешевизне. Большинство телефонных «закладок» автоматически включаются при поднятии телефонной трубки и передают разговор по радиоканалу на приемник пункта перехвата, где он может быть прослушан и записан. Такие «закладки» используют микрофон телефонного аппарата и не имеют своего источника питания, поэтому их размеры могут быть очень небольшими. Часто в качестве антенны используется телефонная линия. Для маскировки телефонные «закладки» выпускаются в виде конденсаторов, реле, фильтров и других стандартных элементов и узлов, входящих в состав телефонного аппарата.

Чаще всего телефонные «закладки» стараются устанавливать за пределами офиса или квартиры, что существенно снижает риск. Для упрощения процедуры подключения подслушивающих устройств и уменьшения влияния на телефонную линию используются изделия с индуктивным датчиком съема информации. Особенностью подобных устройств является то, что требуется автономный источник питания

и устройство должно иметь схему автоматического включения при снятии телефонной трубки. Качество перехватываемой информации практически всегда хуже.

Использование телефонных линий для дистанционного съема аудио-информации из контролируемых помещений

Отдельное место занимают системы, которые предназначены не для подслушивания телефонных переговоров, а для использования телефонных линий при прослушивании контролируемых помещений, где установлены телефонные аппараты или проложены провода телефонных линий. Примером такого устройства может служить «телефонное ухо». «Телефонное ухо» представляет собой небольшое устройство, которое подключается параллельно к телефонной линии или розетке в любом удобном месте контролируемого помещения. Для прослушивания помещения необходимо набрать номер абонента, в помещении которого стоит «телефонное ухо». Услышав первый гудок АТС, необходимо положить трубку и через 10–15 с повторить набор номера. Устройство дает ложные гудки «занято» в течение 40–60 с, после чего гудки прекращаются и включается микрофон в устройстве «телефонное ухо» — начинается прослушивание помещения. В случае обычного звонка «телефонное ухо» пропускает все звонки после первого, выполняя роль обычной телефонной розетки и не мешая разговору.

Кроме того, возможно использование телефонной линии для передачи информации с микрофона, скрытно установленного в помещении. При этом используется несущая частота в диапазоне от десятков до сотен килогерц с целью не препятствовать нормальной работе телефонной связи. Практика показывает, что в реальных условиях дальность действия подобных систем с приемлемой разборчивостью речи существенно зависит от качества линии, прокладки телефонных проводов, наличия в данной местности радиотрансляционной сети, наличия вычислительной и оргтехники и т. д.

Из числа так называемых «беззаходовых» систем съема речевой информации с контролируемых помещений, когда используются телефонные линии, следует отметить возможность съема за счет электроакустического преобразования, возникающего в телефонных аппаратах и за счет высокочастотного (ВЧ) навязывания. Но эти каналы утечки используются все реже. Первый из-за того, что современные телефонные аппараты не имеют механических звонков и крупных металлических деталей, а второй из-за своей сложности и громоздкости аппаратуры. Но, тем не менее, меры защиты от утечки информации по этим каналам применяются, они общеизвестны и недороги.

Использование сети 220 В для передачи акустической информации из помещений

Для этих целей применяют так называемые сетевые «закладки». К этому типу «закладок» чаще всего относят устройства, которые встраиваются в приборы, питающиеся от сети 220 В или сетевую арматуру (розетки, удлинители и т. д.). Передающее устройство состоит из микрофона, усилителя и собственно передатчика несущей низкой частоты. Частота несущей частоты обычно используется в диапазоне от 10 до 350 кГц. Передача и прием осуществляется по одной фазе или, если фазы разные, то их связывают по высокой частоте через разделительный конденсатор. Приемное устройство может быть изготовлено специально, но иногда применяют доработанные блоки бытовых переговорных устройств, которые сейчас продаются во многих специализированных магазинах электронной техники. Сетевые передатчики подобного класса легко камуфлируются под различного рода электроприборы, не требуют дополнительного питания от батарей и трудно обнаруживаются при использовании поисковой аппаратуры, широко применяемой в настоящее время.

§ 2. Технические каналы утечки акустической (речевой) информации

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте. Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т. д. То есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах. В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды, Например, воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт (земля) и т. п. Технические средства разведки служат для приема и измерения параметров сигналов. Под акустической понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой. Акустический сигнал представляет собой возмущения упругой среды, проявляющиеся в возникновении акустических колебаний различной формы и длительности. Акустическими называются механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины.

Первичными источниками акустических колебаний являются механические колебательные системы, например, органы речи человека, а вторичными — преобразователи различного типа, в том числе электроакустические. Последние представляют собой устройства, предназначенные для преобразования акустических колебаний в электрические и обратно. К ним относятся пьезоэлементы, микрофоны, телефоны, громкоговорители и другие устройства. В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Тональный — это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает целый спектр гармонических составляющих. Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200...300 Гц до 4...6 кГц. В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронный и параметрические.

Воздушные технические каналы утечки информации. В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны. Миниатюрные микрофоны объединяются (или соединяются) с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками. Автономные устройства, конструкционно объединяющие миниатюрные микрофоны и передатчики, называют закладными устройствами перехвата речевой информации, или просто акустическими закладками. Перехваченная закладными устройствами речевая информация может передаваться по радиоканалу,

оптическому каналу (в инфракрасном диапазоне длин волн), по сети переменного тока, соединительным линиям вспомогательных технических средств и систем (ВТСС), посторонним проводникам (трубам водоснабжения и канализации, металлоконструкциям и т. п.). Причем для передачи информации по трубам и металлоконструкциям могут использоваться не только электромагнитные, но и механические ультразвуковые колебания. Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн. Однако встречаются закладные устройства, прием информации с которых можно осуществлять с обычного телефонного аппарата. Такие устройства устанавливаются или непосредственно в корпусе телефонного аппарата, находящегося в контролируемом помещении и называемом «телефоном-наблюдателем», или подключаются к телефонной линии, чаще всего в телефонной розетке. Подобное устройство конструкционно объединяет миниатюрный микрофон и специальный блок коммутации и часто называется «телефонным ухом». Блок коммутации подключает микрофон к телефонной линии при дозвоне по определенной схеме до «телефона-наблюдателя» или подаче в линию специального кодированного сигнала. Использование портативных диктофонов и акустических закладок требует проникновения на контролируемый объект (в помещение). В том случае, когда это не удается, для перехвата речевой информации используются направленные микрофоны.

Вибрационные технические каналы утечки информации. В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы). Контактные микрофоны, соединенные с электронным усилителем, называют электронными стетоскопами. По вибрационному каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС. обладающие «микрофонным эффектом», а также путем «высокочастотного навязывания». 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 и 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 из-

менения 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 подключения к соединительным линиям ВТСС, обладающих «микрофонным эффектом», специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты. Технический канал утечки информации путем «высокочастотного навязывания» может быть осуществлен 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. Информационный сигнал в данных элементах ВТСС появляется 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 используется специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы. Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. Для исключения воздействия высокочастотного сигнала на аппаратуру АТС в линию, идущую в ее сторону, устанавливается специальный высокочастотный фильтр.

Оптико-электронный технический канал утечки информации. Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле 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. Причем, лазер и приемник оптического излучения могут быть установлены в одном или разных местах (помещениях). Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы, иногда называемые «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне волн.

Параметрические технические каналы утечки информации. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСГШ и 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, напри-

мер, 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 излучения 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.

Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки. Параметрический канал утечки информации может быть реализован и путем «высокочастотного облучения» помещения, где установлены полуактивные закладные устройства, имеющие элементы, некоторые параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются по закону изменения акустического (речевого) сигнала.

При облучении мощным высокочастотным сигналом помещения, в котором установлено такое закладное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т. е. переизлучение электромагнитного поля. А специальное устройство закладки (например, объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала. Подобного вида закладки иногда называют полуактивными. Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленной антенной и приемник.

Перехват акустических сигналов по воздушным техническим каналам утечки информации осуществляется:

- микрофонами, комплексированными с портативными устройствам и звукозаписи;
- направленными микрофонами;
- микрофонами, комплексированными с устройствами передачи информации по радиоканалу;
- микрофонами, комплексированными с устройствами передачи информации по сети электропитания 220 В;
- микрофонами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне длин волн;
- микрофонами, комплексированными с устройствами передачи информации по телефонной линии;
- микрофонами, комплексированными с устройствами их подключения к телефонной линии («телефону-наблюдателю») по сигналам вызова от внешнего телефонного абонента;
- микрофонами, комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям и т. п.

Перехват акустических сигналов по вибрационным техническим каналам утечки информации осуществляется:

- электронными стетоскопами;
- стетоскопами, комплексированными с устройствами передачи информации по радиоканалу;
- стетоскопами, комплексированными с устройствами передачи информации по оптическому каналу в ИК-диапазоне длин волн;
- стетоскопами, комплексированными с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям и т. п.

Наблюдение тоже дает ценную конфиденциальную информацию, особенно если оно сопряжено с копированием документации, чертежей, образцов продукции и т. д. В принципе, процесс наблюдения сложен, так как требует значительных затрат сил, времени и средств. Поэтому его ведут, как правило, выборочно, это значит, в определенном месте, в определенное время, специально подготовленными людьми и с помощью технических средств. Например, ***волоконно-оптическая система типа РК-1715*** имеет кабель длиной до двух метров. Она позволяет проникать в помещения через замочные скважины, кабельные и отопительные вводы, вентиляционные шахты, фальшпотолки и другие отверстия. Угол обзора системы — 65°, фокусировка — от 10 мм до бесконечности. Работает при слабом освещении. С ее помощью можно читать и фотографировать документы на столах, заметки в настольных календарях, настенные таблицы и диаграммы, считывать информацию с дисплеев. Фотосъемка осуществляется с помощью современной аппаратуры при дневном освещении и ночью, на сверхблизком расстоянии и на удалении до нескольких километров, в видимом свете и в инфракрасном диапазоне (в последнем случае можно выявить исправления, подделки, а также прочесть текст на обгоревших документах). Известны телеобъективы размером всего со спичечный коробок, однако четко снимающие печатный текст на расстояниях до 100 м. А миниатюрная фотокамера в наручных часах (типа РК-420) позволяет делать 7 кадров на одной кассете с расстояния от 1 м и далее без наводки на резкость, установки выдержки, диафрагмы и пр.

§ 3. Планирование защитных мероприятий по видам дестабилизирующего воздействия

Для защиты от несанкционированного доступа, который приводит к дестабилизирующему воздействию, нужно использовать технические средства защиты информации и придерживаться правил безопасности.

Организационные мероприятия — это мероприятия ограничительного характера, сводящиеся в основном, к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

В общем плане организационные мероприятия предусматривают проведение следующих действий:

1) определение границ охраняемой зоны (территории);

2) определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории;

3) определение «опасных», с точки зрения возможности образования каналов утечки информации, технических средств и конструктивных особенностей зданий и сооружений;

4) выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников;

5) реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами.

Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.

На этапе проведения организационных мероприятий необходимо:

- определить перечень сведений с ограниченным доступом, подлежащих технической защите (определяет собственник информации в соответствии с действующим законодательством Российской Федерации);
- обосновать необходимость разработки и реализации защитных мероприятий с учетом материального или иного ущерба, который может быть нанесен вследствие возможного нарушения целостности информации либо ее утечки по техническим каналам;
- установить перечень выделенных помещений, в которых не допускается реализация угроз и утечка информации с ограниченным доступом;
- определить перечень технических средств, которые должны использоваться как основные технические средства (ОТС);
- определить технические средства, применение которых не обосновано служебной и производственной необходимостью и которые подлежат демонтажу;
- определить наличие задействованных и незадействованных воздушных, наземных, настенных и заложенных в скрытую канализацию кабелей, цепей и проводов, уходящих за пределы выделенных помещений;
- определить системы, подлежащие демонтажу, требующие переоборудования кабельных сетей, цепей питания, заземления или установки в них защитных устройств. Подготовительные технические мероприятия включают в себя первичные меры блокирования электроакустических преобразователей и линий связи, выходящих за пределы выделенных помещений. Блокирование линий связи может выполняться следующими способами:
- отключением линий связи ТСПИ и ВТСС или установкой простейших схем защиты;
- демонтажем отдельных технических средств, кабелей, цепей, проводов, уходящих за пределы выделенных помещений;

- удалением за пределы выделенных помещений отдельных элементов технических средств, которые могут являться источником возникновения канала утечки информации.

Блокирование каналов возможной утечки информации ограниченного доступа (ИОД) в системах городской и ведомственной телефонной связи может осуществляться:

- отключением звонковых (вызывных) линий телефонного аппарата;
- установкой в цепи телефонного аппарата безразрывной розетки для временного отключения;
- установкой простейших устройств защиты.

Защита информации от утечки через радиотрансляционную сеть, выходящую за пределы выделенного помещения, может быть обеспечена:

- отключением громкоговорителей по двум проводам;
- включением простейших устройств защиты.

Для службы оповещения следует выделить дежурные абонентские устройства вне выделенных помещений; цепи к этим устройствам должны быть проложены отдельным кабелем.

Предотвращение утечки информации через системы пожарной и охранной сигнализаций осуществляется отключением датчиков пожарной и охранной сигнализации на период проведения важных мероприятий, содержащих ИОД, или применением датчиков, не требующих специальных мер защиты.

Блокирование утечки ИОД через системы электронной оргтехники и кондиционирования может быть обеспечено следующими мерами:

- расположением указанных систем внутри контролируемой территории без выноса отдельных компонентов за ее пределы;
- электропитанием систем от трансформаторной подстанции, находящейся внутри контролируемой территории.

При невыполнении указанных выше условий системы должны отключаться от сети электропитания по двум проводам.

Защита ИОД от утечки через цепи электроосвещения и электропитания бытовой техники должна осуществляться подключением указанных цепей к отдельному фидеру трансформаторной подстанции, к которому не допускается подключение сторонних пользователей.

В случае невыполнения указанного требования электробытовые приборы на период проведения закрытых мероприятий должны отключаться от цепей электропитания.

Технические мероприятия — это мероприятия, обеспечивающие приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений (безопасных) технических средств или средств, ПЭМИН которых не превышают границу охраняемой территории.

Технические мероприятия по защите конфиденциальной информации можно подразделить на скрытие, подавление и дезинформацию.

Скрытие выражается в использовании радиомолчания и создании пассивных помех приемным средствам злоумышленников.

Подавление — это создание активных помех средствам злоумышленников.

Дезинформация — это организация ложной работы технических средств связи и обработки информации; изменение режимов использования частот и регламентов связи; показ ложных демаскирующих признаков деятельности и опознавания.

Защитные меры технического характера могут быть направлены на конкретное техническое устройство или конкретную аппаратуру и выражаются в таких мерах, как отключение аппаратуры на время ведения конфиденциальных переговоров или использование тех или иных защитных устройств типа ограничителей, буферных средств, фильтров и устройств зашумления.

Технические мероприятия являются основным этапом работ по технической защите информации ограниченного доступа и заключаются в установке основных технических средств, обеспечении ТСПИ и ВТСС устройствами технической защиты информации. При выборе, установке, замене технических средств следует руководствоваться прилагаемыми к этим средствам паспортами, техническими описаниями, инструкциями по эксплуатации, рекомендациями по установке, монтажу и эксплуатации.

ОТС должны размещаться, по возможности, ближе к центру здания или в сторону наибольшей части контролируемой территории. Составные элементы ОТС должны размещаться в одном помещении либо в смежных. К средствам технической защиты относятся:

- фильтры-ограничители и специальные абонентские устройства защиты для блокирования утечки речевой ИОД через двухпроводные линии телефонной связи, системы директорской и диспетчерской связи;
- устройства защиты абонентских однопрограммных громкоговорителей для блокирования утечки речевой ИОД через радиотрансляционные линии;
- фильтры сетевые для блокирования утечки речевой ИОД по цепям электропитания переменного (постоянного) тока;
- фильтры защиты линейные (высокочастотные) для установки в линиях аппаратов телеграфной (телекодовой) связи;
- генераторы линейного зашумления;
- генераторы пространственного зашумления;
- экранированные камеры специальной разработки.

Для телефонной связи, предназначенной для передачи ИОД, рекомендуется применять аппараты отечественного производства, совместимые с устройствами защиты. Телефонные аппараты иностранного производства могут применяться при условии прохождения специсследований и положительного заключения компетентных организаций системы ТЗИ об их совместимости с устройствами защиты. Выбор методов и способов защиты элементов ТСПИ и ВТСС, обладающих микрофонным эффектом, зависит от величины их входного сопротивления на частоте 1 кГц. Элементы с входным сопротивлением менее 600 Ом (головки громкоговорителей, электродвигатели вентиляторов, трансформаторы и т. п.) рекомендуется отключать по двум проводам или устанавливать в разрыв цепей устройства защиты с высоким выходным сопротивлением для снижения до минимальной величины информативной составляющей тока. Элементы с высоким входным сопротивлением (электрические звонки, телефонные капсюли, электромагнитные реле) рекомендуется не только отключать от цепей, но и замыкать на низкое сопротивление или закорачивать, чтобы уменьшить электрическое поле от данных элементов, обусловленное напряжением, наведенным при воздействии акустического поля. При этом следует учитывать, что выбранный способ защиты не должен нарушать работоспособность технического средства и ухудшать его технические параметры. Высокочастотные автогенераторы, усилители (микрофонные, приема, передачи, громкоговорящей связи) и другие устройства, содержащие активные элементы, рекомендуется отключать от линий электропитания в «дежурном режиме» или «режиме ожидания вызова». Защиту ИОД от утечки по кабелям и проводам рекомендуется осуществлять путем:

- применения экранирующих конструкций;
- раздельной прокладки кабелей ОТС, ТСПИ и ВТСС.

При невозможности выполнения требований по разносу кабелей электропитания ОТС, ТСПИ и ВТСС электропитание последних следует осуществлять либо экранированными кабелями, либо от разделительных систем, либо через сетевые фильтры. Не допускается образование петель и контуров кабельными линиями. Пересечение кабельных трасс разного назначения рекомендуется осуществлять под прямым углом друг к другу. Электропитание ОТС должно быть стабилизировано по напряжению и току для нормальных условий функционирования ОТС и обеспечения норм защищенности. В цепях выпрямительного устройства источника питания необходимо устанавливать фильтры нижних частот. Фильтры должны иметь фильтрацию по симметричным и несимметричным путям распространения.

Необходимо предусмотреть отключение электросети от источника питания ОТС при исчезновении напряжения в сети, при отклонении параметров электропитания от норм, заданных в ТУ, и при появлении неисправностей в цепях электропитания. Все металлические конструкции ОТС (шкафы, пульты, корпуса распределительных устройств и металлические оболочки кабелей) должны быть заземлены. Заземление ОТС следует осуществлять от общего контура заземления, размещенного в пределах контролируемой территории, с сопротивлением заземления по постоянному току в соответствии с требованиями стандартов. Система заземления должна быть единой для всех элементов ОТС и строиться по радиальной схеме. Образование петель и контуров в системе заземления не допускается. Экраны кабельных линий ОТС, выходящих за пределы контролируемой территории, должны заземляться в кроссах от общего контура заземления в одной точке для исключения возможности образования петель по экрану и корпусам. В каждом устройстве должно выполняться условие непрерывности экрана от входа до выхода. Экраны следует заземлять только с одной стороны. Экраны кабелей не должны использоваться в качестве второго провода сигнальной цепи или цепи питания. Экраны кабелей не должны иметь электрического контакта с металлоконструкциями. Для монтажа следует применять экранированные кабели с изоляцией или надевать на экраны изоляционную трубку. В длинных экранированных линиях (микрофонных, линейных, звукоусилительных) рекомендуется делить экран на участки для получения малых сопротивлений для высокочастотных токов и каждый участок заземлять только с одной стороны.

Любое техническое устройство вносит какие-то изменения в окружающее пространство. И если задача разведки состоит в том, чтобы сделать эти изменения как можно более незаметными, то задача тех, кто занят поиском подобной техники, состоит в том, чтобы по едва уловимым следам изменения физических параметров пространства обнаружить и обезвредить технические устройства и системы ведения разведки. Задача технической контрразведки усложняется тем, что, как правило, неизвестно, какое конкретное техническое устройство контроля информации применено. Поэтому работа по поиску и обезвреживанию технических средств наблюдения дает обнадеживающий результат только в том случае, если она проводится комплексно, т. е. обследуют одновременно все возможные пути утечки информации. Приведем достаточно условную классификацию устройств поиска технических средств разведки:

1. *Устройства поиска активного типа,* т. е. исследующие отклик на какое-либо воздействие:

– нелинейные локаторы — исследуют отклик на воздействие электромагнитным полем;

– рентгенметры — просвечивание с помощью рентгеновской аппаратуры;
– магнитно-резонансные локаторы, использующие явление ориентации молекул в магнитном поле;
– акустические корректоры.

2. *Устройства поиска пассивного типа:*
– металлоискатели;
– тепловизоры;
– устройства и системы поиска по электромагнитному излучению;
– устройства поиска по изменению параметров телефонной линии (напряжения, индуктивности, емкости, добротности);
– устройства поиска по изменению магнитного поля (детекторы записывающей аппаратуры).

В силу различных причин практическое применение нашли далеко не все из перечисленных технических средств. Например, рентгеновская аппаратура очень дорога и громоздка и применяется исключительно специальными государственными организациями. То же, но в меньшей степени, относится к магнитно-резонансным локаторам. Тепловизоры, приборы, которые могут обнаруживать разницу температур, измеряемую сотыми долями градуса, могут регистрировать тепловую мощность порядка 1 мкВт. Эти относительно дешевые приборы, в состав которых входит компьютер, могли бы стать очень эффективными и универсальными с точки зрения поиска технических средств коммерческой разведки, т. к. любое техническое средство при своей работе выделяет в окружающее пространство тепло. Скорее всего, появление на рынке подобных устройств является делом недалекого будущего.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний. Для этих целей необходима работа сотрудников службы безопасности с информаторами в интересах наблюдения и объективной оценки ситуации как внутри коллектива сотрудников, так и вне, среди конкурентов и преступных формирований.

Обнаружение угроз — это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов. В числе мероприятий по обнаружению угроз значительную роль могут сыграть не только сотрудники СБ, но и сотрудники линейных подразделений и служб, а также технические средства наблюдения и обнаружения правонарушений.

Пресечение или локализация угроз — это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков.

Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

1) предотвращение разглашения и утечки конфиденциальной информации;
2) воспрещение несанкционированного доступа к источникам конфиденциальной информации; сохранение целостности, полноты и доступности информации;
3) соблюдение конфиденциальности информации;
4) обеспечение авторских прав.

Защита от разглашения сводится в общем плане к разработке перечня сведений, составляющих информацию ограниченного доступа. Эти сведения должны быть доведены до каждого сотрудника, допущенного к ним, с обязательством этого сотрудника сохранять служебную или государственную тайну.

Защита от утечки конфиденциальной информации сводится к выявлению, учету и контролю возможных каналов утечки в конкретных условиях и к проведению организационных, организационно-технических и технических мероприятий по их ликвидации.

Защита от несанкционированного доступа к конфиденциальной информации обеспечивается путем выявления, анализа и контроля возможных способов несанкционированного доступа и проникновения к источникам конфиденциальной информации и реализацией организационных, организационно-технических и технических мероприятий по противодействию НСД.

На практике в определенной степени все мероприятия по использованию технических средств защиты информации подразделяются на три группы:

1) организационные (в части технических средств);
2) организационно-технические;
3) технические.

Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфиденциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств, устанавливаемых на элементы конструкций зданий, помещений и технических средств, потенциально образующих каналы утечки информации. В этих целях возможно использование:

- технических средств пассивной защиты, например фильтров, ограничителей и тому подобных средств развязки акустических, электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, радиоикации и др.;
- технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.

Организационно-технические мероприятия по защите информации можно подразделить на пространственные, режимные и энергетические.

Пространственные меры выражаются в уменьшении ширины диаграммы направленности, ослаблении боковых и заднего лепестков диаграммы направленности излучения радиоэлектронных средств (РЭС).

Режимные меры сводятся к использованию скрытых методов передачи информации по средствам связи: шифрование, квазипеременные частоты передачи и др.

Энергетические — это снижение интенсивности излучения и работа РЭС на пониженных мощностях.

§ 4. Средства защиты информации в автоматизированных системах

Все средства защиты информации (СЗИ) условно можно разделить на несколько групп:

- средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
- средства, обеспечивающие защиту информации при передаче ее по каналам связи;
- средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
- средства, обеспечивающие защиту от воздействия программ-вирусов;
- материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Основное назначение средств защиты первой группы — разграничение доступа к локальным и сетевым информационным ресурсам автоматизированных систем. СЗИ этой группы обеспечивают:

- идентификацию и аутентификацию пользователей автоматизированных систем;
- разграничение доступа зарегистрированных пользователей к информационным ресурсам;
- регистрацию действий пользователей;
- защиту загрузки операционной системы с гибких магнитных дисков и CD-ROM;
- контроль целостности СЗИ и информационных ресурсов.

В качестве идентификаторов пользователей применяются, как правило, условные обозначения в виде набора символов. Для аутентификации пользователей применяются пароли.

Ввод значений идентификатора пользователя и его пароля осуществляется по запросу СЗИ с клавиатуры. Многие современные СЗИ используют и другие типы идентификаторов — магнитные карточки, радиочастотные бесконтактные карточки, смарт-карточки, электронные таблетки Touch Memory и другие. Отдельно стоит сказать об использовании в качестве идентификатора индивидуальных биологических параметров (отпечаток пальца, радужная оболочка глаза), присущих каждому человеку. Использование в качестве идентификаторов индивидуальных биологических параметров характеризуется, с одной стороны, высшим уровнем конфиденциальности, а с другой — очень высокой стоимостью таких систем. Разграничение доступа зарегистрированных пользователей к информационным ресурсам осуществляется СЗИ в соответствии с установленными для пользователей полномочиями. Как правило, СЗИ обеспечивают разграничение доступа к гибким и жестким дискам, логическим дискам, директориям, файлам, портам и устройствам. Полномочия пользователей устанавливаются с помощью специальных настроек СЗИ. По отношению к информационным ресурсам средствами защиты могут устанавливаться такие полномочия, как разрешение чтения, записи, создания, запуска исполняемых файлов и другие. Системы защиты информации предусматривают ведение специального журнала, в котором регистрируются определенные события, связанные с действиями пользователей, например запись (модификация) файла, запуск программы, вывод на печать и другие, а также попытки несанкционированного доступа к защищаемым ресурсам и их результат. Особо стоит отметить наличие в СЗИ защиты загрузки операционной системы с гибких магнитных дисков и CD-ROM, которая обеспечивает за-

щиту самих средств защиты от «взлома» с использованием специальных технологий. В различных СЗИ существуют программные и аппаратно-программные реализации этой защиты, однако практика показывает, что программная реализация не обеспечивает необходимой стойкости. Контроль целостности средств защиты и защищаемых файлов заключается в подсчете и сравнении контрольных сумм файлов. При этом используются различной сложности алгоритмы подсчета контрольных сумм. Несмотря на функциональную общность средств защиты информации данной группы, СЗИ различных производителей различаются:

- условиями функционирования (операционная среда, аппаратная платформа, автономные компьютеры и вычислительные сети);
- сложностью настройки и управления параметрами СЗИ;
- используемыми типами идентификаторов;
- перечнем событий, подлежащих регистрации;
- стоимостью средств защиты.

С развитием сетевых технологий появился новый тип СЗИ — межсетевые экраны (*firewalls*), которые обеспечивают решение таких задач, как защита подключений к внешним сетям, разграничение доступа между сегментами корпоративной сети, защита корпоративных потоков данных, передаваемых по открытым сетям. Защита информации при передаче ее по каналам связи осуществляется средствами криптографической защиты (СКЗИ). Характерной особенностью этих средств является то, что они потенциально обеспечивают наивысшую защиту передаваемой информации от несанкционированного доступа к ней. Помимо этого, СКЗИ обеспечивают защиту информации от модификации (использование цифровой подписи и имитовставки). Как правило, СКЗИ функционируют в автоматизированных системах как самостоятельное средство, однако в отдельных случаях СКЗИ может функционировать в составе средств разграничения доступа как функциональная подсистема для усиления защитных свойств последних. Обеспечивая высокую степень защиты информации, в то же время применение СКЗИ влечет ряд неудобств:

- стойкость СКЗИ является потенциальной, т. е. гарантируется при соблюдении ряда дополнительных требований, реализация которых на практике осуществляется довольно сложно (создание и функционирование ключевой системы, распределение ключей, обеспечение сохранности ключей, необходимость в получении лицензии на право эксплуатации средств, планирование и организация мероприятий при компрометации ключевой системы);
- относительно высокая стоимость эксплуатация таких средств.

В целом, при определении необходимости использования средств криптографической защиты информации, необходимо учитывать то, что применение СКЗИ оправдано в случаях явного перехвата действительно конфиденциальной информации. Для защиты информации от утечки по физическим полям используются следующие методы и средства защиты:

- электромагнитное экранирование устройств или помещений, в которых расположена вычислительная техника;
- активная радиотехническая маскировка с использованием широкополосных генераторов шумов, которые широко представлены на нашем рынке.

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

И несколько слов о материалах, обеспечивающих безопасность хранения, транспортировки носителей информации и защиту их от копирования. В основном это специальные тонкопленочные материалы с изменяющейся цветовой гаммой или голографические метки, которые наносятся на документы и предметы (в том числе и на элементы компьютерной техники автоматизированных систем). Они позволяют:

- идентифицировать подлинность объекта;
- контролировать несанкционированный доступ к ним.

Защита телефонных линий. Среди всего многообразия способов несанкционированного перехвата информации особое место занимает прослушивание телефонных переговоров, поскольку телефонная линия — самый первый, самый удобный и при этом самый незащищенный источник связи между абонентами в реальном масштабе времени. На заре развития телефонной связи никто особо не задумывался о защите линий от прослушивания, и электрические сигналы распространялись по проводам в открытом виде. В наше время микроэлектронной революции прослушать телефонную линию стало простым и дешевым делом. Можно уверенно заявить о том, что если злоумышленник принял решение о «разработке» объекта, то первое, что он, скорее всего, сделает, это начнет контроль телефонных переговоров. Его можно осуществлять, не заходя в помещение, при минимальных затратах и минимальном риске. Нужно просто подключить к телефонной линии объекта специальное приемно-передающее или регистрирующее устройство. С точки зрения безопасности телефонная связь имеет еще один недостаток: возможность перехвата речевой информации из помещений, по которым проходит телефонная линия и где подключен телефонный аппарат. Это осуществимо даже тогда, когда не ведутся телефонные переговоры (так называемый микрофонный эффект телефона и метод высокочастотного (ВЧ) навязывания). Для такого перехвата существует специальное оборудование, которое подключается к телефонной линии внутри контролируемого помещения или даже за его пределами. Для защиты обычных городских телефонных каналов сегодняшний официальный рынок представляет пять разновидностей специальной техники:

- криптографические системы защиты (для краткости — скремблеры);
- анализаторы телефонных линий;
- односторонние маскираторы речи;
- средства пассивной защиты;
- постановщики активной заградительной помехи.

Защита сети питания и заземления. Для фильтрации сигналов в цепях питания технических средств передачи информации (ТСПИ) используются разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные трансформаторы. Такие трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками. Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю. Однако электростатическое поле вокруг экрана также может служить причиной проникновения наводок во вторичную цепь. Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

- разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;
- устранения асимметричных наводок;
- ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

Средства развязки и экранирования, применяемые в разделительных трансформаторах, обеспечивают максимальное значение сопротивления между обмотками и создают для наводок путь с малым сопротивлением из первичной обмотки на землю. Это достигается обеспечением высокого сопротивления изоляции соответствующих элементов конструкции (~10^4 МОм) и незначительной емкости между обмотками. Указанные особенности трансформаторов для цепей питания обеспечивают более высокую степень подавления наводок, чем обычные трансформаторы. Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивает ослабление информационного сигнала наводки в нагрузке на 126 дБ при емкости между обмотками 0,005 пФ и на 140 дБ при емкости между обмотками 0,001 пФ. Средства экранирования, применяемые в разделительных трансформаторах, должны не только устранять влияние асимметричных наводок на защищаемое устройство, но и не допустить на выходе трансформатора симметричных наводок, обусловленных асимметричными наводками на его входе. Применяя в разделительных трансформаторах специальные средства экранирования, можно существенно (более чем на 40 дБ) уменьшить уровень таких наводок.

Помехоподавляющие фильтры. В настоящее время существует большое количество различных типов фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Это фильтры нижних и верхних частот, полосовые и заграждающие фильтры и т. д. Основное назначение фильтров — пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы. Для исключения просачивания информационных сигналов в цепи электропитания используются фильтры нижних частот.

Фильтр нижних частот (ФНЧ) пропускает сигналы с частотами ниже граничной частоты ($f \le frp$) и подавляет — с частотами выше граничной частоты.

Последовательная ветвь ФНЧ должна иметь малое сопротивление для постоянного тока и нижних частот. Вместе с тем для того, чтобы высшие частоты задерживались фильтром, последовательное сопротивление должно расти с частотой. Этим требованиям удовлетворяет индуктивность L. Параллельная ветвь ФНЧ, наоборот, должна иметь малую проводимость для низких частот с тем, чтобы токи этих частот не шунтировались параллельным плечом. Для высоких частот параллельная ветвь должна иметь большую проводимость, тогда колебания этих частот будут ею шунтироваться, и их ток на выходе фильтра будет ослабляться. Таким требованиям отвечает емкость С. Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

- величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;
- величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой;
- ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным;
- габариты и масса фильтров должны быть минимальными;

• фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т. д.);

• конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими, предъявляются следующие дополнительные требования:

• затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10 ГГц);

• сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний;

• ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Конструктивно фильтры подразделяются на:

• фильтры на элементах с сосредоточенными параметрами (LC-фильтры) — обычно предназначены для работы на частотах до 300 МГц;

• фильтры с распределенными параметрами (полосковые, коаксиальные или волноводные) — применяются на частотах свыше 1 ГГц;

• комбинированные — применяются на частотах 300 МГц ... 1 ГГц.

В настоящее время промышленностью выпускаются несколько серий защитных фильтров (ФП, ФБ, ФПС и др.).

Фильтры серии ФП обеспечивают затухание от 60 до 100 дБ. Они рассчитаны на номинальное напряжение переменного тока от 60 до 500 В и ток — от 2,5 до 70 А. Размеры фильтров составляют от $350 \times 100 \times 60$ до $560 \times 210 \times 80$ мм, а вес — от 2,5 до 25 кг.

Фильтры серии ФСПК-100 (200) предназначены для установки в четырехпроводных линиях электропитания частотой 50 Гц и напряжением 220/380 В. Максимальный рабочий ток составляет 100 (200) А. В диапазоне частот от 0,02 до 1000 МГц фильтры обеспечивают затухание сигнала не менее 60 дБ. Конструктивно фильтры ФСПК выполнены в виде двух корпусов (полукомплектов), каждый из которых обеспечивает фильтрацию двухпроводной линии. Размеры одного корпуса составляют $800 \times 320 \times 92$ мм, а вес — 18 кг. Необходимо помнить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств. В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемы. На рисунке 7.4.1 представлена одноточечная последовательная схема заземления.

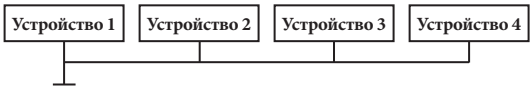


Рисунок 7.4.1 — Одноточечная последовательная схема заземления

Эта схема наиболее проста. Однако ей присущ недостаток, связанный с протеканием обратных токов различных цепей по общему участку заземляющей цепи. Вследствие этого возможно появление опасного сигнала в посторонних цепях. В одноточечной параллельной схеме заземления этого недостатка нет (рис. 7.4.2). Однако такая схема требует большого числа протяженных заземляющих проводников, из-за чего может возникнуть проблема с обеспечением малого сопротивления заземления участков цепи. Кроме того, между заземляющими проводниками могут возникать нежелательные связи, которые создают несколько путей заземления для каждого устройства. В результате в системе заземления могут возникнуть уравнительные токи и появиться разность потенциалов между различными устройствами.

Рисунок 7.4.2 — Одноточечная параллельная схема заземления

Многоточечная схема заземления практически свободна от недостатков, присущих одноточечной схеме (рис. 7.4.3). В этом случае отдельные устройства и участки корпуса индивидуально заземлены. При проектировании и реализации многоточечной системы заземления необходимо принимать специальные меры для исключения замкнутых контуров.

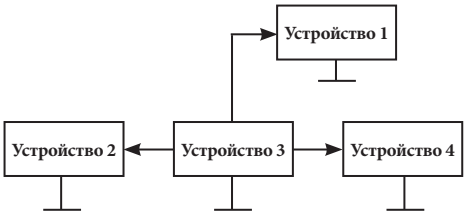


Рисунок 7.4.3 — Многоточечная схема заземления

Как правило, одноточечное заземление применяется на низких частотах при небольших размерах заземляемых устройств и расстояниях между ними менее 0,5λ. На высоких частотах при больших размерах заземляемых устройств и значительных расстояниях между ними используется многоточечная система заземления. В промежуточных случаях эффективна комбинированная (гибридная) система заземления, представляющая собой различные сочетания одноточечной, многоточечной и плавающей заземляющих систем. Заземление технических средств систем информатизации и связи должно быть выполнено в соответствии с определенными правилами. Основные требования, предъявляемые к системе заземления, заключаются в следующем:

- система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;

- сопротивления заземляющих проводников, а также земляных шин должны быть минимальными;
- каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления. Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;
- в системе заземления должны отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;
- следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;
- качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и вибрации;
- контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;
- контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;
- запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, имеющие соединение с землей, металлические оболочки подземных кабелей, металлические трубы систем отопления, водоснабжения, канализации и т. д. На практике наиболее часто в качестве заземлителей применяют:
  - стержни из металла, обладающие высокой электропроводностью, погруженные в землю и соединенные с наземными металлоконструкциями средств ТСПИ;
  - сеточные заземлители, изготовленные из элементов с высокой электропроводностью и погруженные в землю (служат в качестве дополнения к заземляющим стержням).

Защита по виброакустическому каналу утечки информации. Метод съема информации по виброакустическому каналу относится к так называемым беззаходовым методам, и это является важным его преимуществом. Обнаружить аппаратуру такого съема информации крайне трудно, так как она устанавливается за пределами контролируемого помещения, а в ряде случаев существенно удалена от него.

Кратко о физическом принципе, который лежит в основе этого метода. Речь, вызывающая акустические сигналы, представляет собой механические колебания воздушной среды. Попадая на твердые поверхности (стены, перегородки), они преобразуются в структурные вибрационные сигналы, которые, оставаясь по своей природе механическими, распространяется по строительным конструкциям здания. Можно выделить следующие типовые конструкции, по которым передаются речевые сигналы:

- в акустическом сигнале это — несущие стены зданий, перегородки, перекрытия зданий, окна, двери, вентиляционные воздуховоды;
- в вибрационном канале это — стены и перегородки, перекрытия, оконные рамы, дверные коробки, трубопроводы, короба вентиляции.

Если акустические датчики установлены на этих конструкциях за пределами помещения, это дает возможность принять речевые сигналы и проконтролировать раз-

говоры внутри него. При этом необязательно скрытно проникать в помещение — достаточно приблизиться к нему снаружи. Установить датчик можно и дистанционным способом — с помощью специальных выстреливающих устройств. Иногда используют лазерные устройства и направленные микрофоны. Действие лазерных устройств основано на принципе снятия вибрации (речевых сигналов) с оконного стекла, а направленные микрофоны снимают речевую информацию по акустическому каналу.

Для обратного преобразования механических колебаний в акустический сигнал служат контактные микрофоны, известные под названием стетоскопы. Электронные стетоскопы сначала преобразуют механические колебания в электрический сигнал, который затем усиливается и уже тогда преобразуется в акустический. Итак, вибрационным каналом утечки информации здесь уже является не воздух, а другая среда распространения акустического сигнала. Такие каналы возникают при падении первичной акустической волны в воздухе на другую среду и дальнейшем распространении ее в новой среде. На практике это — стены, пол, потолок, двери и косяки, стекла, оконные рамы и коробки, инженерные коммуникации, проходящие или выходящие из помещения. Предотвращение утечки информации по этим каналам сводится, как и в случае с акустическими каналами, к двум направлениям:

1. Максимально ослабить акустический сигнал от источника звука, попадающий в другую среду распространения, где его могут перехватить. Заставить акустическую волну пройти сначала среду с высоким затуханием, например. Это означает, что отделка стен звукопоглощающими материалами предпочтительнее, чем простая оклейка обоями. Тяжелые портьеры на окнах значительно ослабляют акустический сигнал, попадающий на стекла. Красивые дубовые сплошные одинарные двери явно проигрывают по этому параметру двойным, обитым дерматином.

2. Создать в «опасной» среде распространения сильный помеховый сигнал, который невозможно отфильтровать от полезного. Само собой разумеется, что помехи и так есть — бульканье воды в трубах отопления, сверление бетонных стен соседями по дому, шум от проезжающих по улице тяжелых грузовиков и трамваев. Для зашумления используют уже упоминавшиеся генераторы белого шума, к которым подсоединяют специальные излучатели, устанавливаемые на стенах, стеклах, рамах, косяках, трубах отопления и т. д.

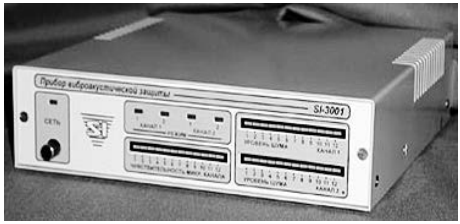
Из всего вышесказанного можно сделать следующие выводы:

- В общем случае акустический сигнал распространяется в упругих средах с затуханием, зависящем от свойств среды распространения.
- При переходе из одной среды в другую часть сигнала теряется (отражение, поглощение).
- Виброакустическими каналами утечки информации является совокупность сред распространения сигнала от источника до приемника.

Прибор виброакустической защиты SI-3001 предназначен для защиты помещений от прослушивания через строительные элементы конструкции. Принцип действия прибора основан на маскировании спектра речи шумовой помехой, излучаемой в стены, перекрытия, окна, воздуховоды, трубы отопления.

В отличие от других генераторов он имеет два независимых канала, что позволяет дифференцированно подходить к конфигурированию ветвей виброакустической защиты. Повышенная выходная мощность каждого канала обеспечивает нормальную работу значительно большего, чем у других моделей, числа излучателей. При этом изделие работает со всеми типами излучателей, имеющимися на рынке. Это очень удобно, если Вы наращиваете или модернизируете свою систему защиты. Еще одной отличительной чертой является генерация наряду с обычным

белым шумом речеподобной помехи, что значительно повышает степень защиты информации. Кроме того, использование речеподобной помехи позволяет снизить уровень шумовой помехи, подводимой к излучателю, что приводит к уменьшению паразитного шума в помещении. Особенностью прибора является также формирование шумовой помехи с автоматически регулируемым уровнем, чем громче Вы говорите, т. е. чем больше опасность перехвата, тем больше уровень шумового сигнала и наоборот.



Основные функциональные возможности прибора:

- Использование двух независимых каналов.
- Прибор имеет возможность подключения виброакустических излучателей отечественного и импортного производства (TRN-2000, OMS-2000, SPP-4.1, КВП и др.).
- Использование внутренней помехи, формируемой встроенным генератором и помехи подаваемой внешним источником сигнала (диктофон, генератор) на линейный вход прибора.
- Режим автоматического регулирования уровня сигнала на выходе прибора пропорционально уровню шума в защищаемом помещении.
- Регулировка уровня выходного сигнала в каждом канале, что позволяет настраивать прибор с разными типами датчиков под конкретные условия эксплуатации.
- Возможность плавной регулировки чувствительности микрофонного канала.
- Благодаря возможности подключения любых типов виброакустических излучателей потребитель может модифицировать имеющуюся систему защиты без демонтажа и замены ранее установленных излучателей.
- Прибор собран на современной импортной элементной базе ведущих фирм изготовителей и не имеет аналогов.

Технические данные и характеристики:

Количество подключаемых излучателей:	
электромагнитных (TRN-2000)	72
керамических (КВП-2)	200
акустических (OMS-2000)	144
пьезоизлучателей (SPP 4.1)	не ограничено
Спектр шумовой помехи	25 Гц ... 5 кГц
Номинальная выходная мощность	70 Вт
Питание прибора электросеть	220 В 50 Гц
Габаритные размеры	200 × 215 × 53 мм

Рекомендуется на одной защищаемой поверхности площадью до 10 кв. м размещать один излучатель. На стеклах допускается приклеивать их в уголках, на стенах — лучше в середине. Если подключить «гирлянду» датчиков-излучателей к прибору и включить его, то, приблизив ухо к защищаемой поверхности, можно услышать характерный шум. Если имеется стетоскоп, то попытка прослушать помещение убедительно покажет невозможность этого. Для обнаружения *радиостетоскопов* можно использовать специальные приборы для обнаружения работающих радиопередатчиков.

«СРМ 700» Многофункциональный поисковый прибор. Портативный многофункциональный прибор СРМ-700 предназначен для выявления и локализации каналов утечки информации в широком диапазоне частот. Являясь одной из основных поисковых систем для комплексной защиты информации, выполняет пять наиболее важных функций:

1. При помощи высокочастотного зонда возможен поиск и обнаружение работающих радиопередатчиков, установленных в предметах интерьера, в одежде, в телефонных аппаратах и других технических средствах обработки и передачи данных. Прибор способен детектировать активизируемые передающие устройства с дистанционным управлением.

2. Низкочастотной антенной можно обследовать электро- и телефонные линии, а также провода электрической сети и кабели, которые могут являться каналами утечки информации.

3. При помощи высокочувствительного усилителя можно исследовать телефонные и другие линии на предмет выявления подключенных к ним микрофонов.

4. В режиме мониторинга прибор может быть использован для фиксации негласного включения передающих устройств с целью снятия информации.

5. Возможно подключение устройства звукозаписи для документирования всех выявленных сигналов.

Многофункциональный поисковый прибор СРМ-700 легок и эффективен в работе благодаря автоматической регулировке усиления, цифровой регулировке режима работы. Благодаря высокой чувствительности, СРМ-700 предназначен для быстрого и бесшумного детектирования всех основных типов электронных средств, предназначенных для скрытого получения информации. Прибор поставляется в атташе-кейсе. В качестве дополнительных аксессуаров предлагаются:

IRP-700 — зонд инфракрасных излучений для обнаружения устройств, использующих ИК-лучи как средство передачи информации;
MLP-700 — зонд электромагнитных излучений;
ALP-700 — акустический зонд;
MPA-700 — телефонный адаптер;
TRP-700 — шнур подключения к магнитофону;
CLA-700 — адаптер питания от прикуривателя автомобиля;
NCB-700 — комплект аккумуляторов;
IRT-700 — тестовый инфракрасный передатчик;
CCT-700 — тестовый низкочастотный (сетевой) передатчик;
TTM-700 — тестовый радиопередатчик.

Технические характеристики:

Диапазон частот ВЧ-антенны	50 кГц — 3 ГГц
Чувствительность ВЧ-антенны	–62 дБ на сегмент индикатора
Коэффициент усиления	20 дБ
Диапазон частот НЧ-зонда	15 кГц — 1 МГц
Чувствительность НЧ-зонда	–38 дБ на сегмент индикатора
Максимальное входное напряжение	300 В
Диапазон звуковых частот	100 Гц — 15 кГц
Система отображения	18-значный ЖКД

Для обнаружения *стетоскопов с прямой записью на диктофон* используют приборы для поиска диктофонов.

«PTRD-018» Стационарный обнаружитель диктофонов

PTRD-018 (Portable tape recorder detector) — современная микропроцессорная система для защиты помещений от несанкционированного использования портативных звукозаписывающих устройств — диктофонов и им подобной аппаратуры. Система обеспечивает обнаружение работающего в режиме записи диктофона, определение его местоположения и времени работы с выводом текущей информации на ЖК-дисплей, либо через интерфейс RS-232 на экран монитора компьютера. Имеет раздельную индикацию по 16 независимым каналам, что позволяет более качественно оценивать угрозу несанкционированного применения звукозаписывающей аппаратуры.

Преимущества системы:

- Возможность обнаружения диктофонов в большом помещении — охват до 16 мест размеров порядка 1 × 1 м.
- Автоматическая адаптация к электромагнитной обстановке контролируемого помещения.
- Высокая защищенность от вибраций и электромагнитных помех.
- Применение жидкокристаллического дисплея обеспечивает наглядность результатов контроля: отображается номер канала, уровень сигнала, сообщение о тревоге.
- Обеспечение протоколирования результатов: все тревожные события, произошедшие за время сеанса контроля, заносятся в протокол с указанием номера канала, частоты сигнала, его уровня, времени включения и выключения.
- Возможность выбора режимов работы в зависимости от поставленной задачи: «быстрее» или «дальше».
- Возможность подключения к компьютеру позволяет интегрировать PTRD-018 в общую систему безопасности.

Принцип действия:

Основой построения системы является регистрация электромагнитных полей, создаваемых работающим мотором диктофонов. При появлении в контролируемой зоне работающего диктофона, он обнаруживается системой и индицируется сигналом тревоги. Контроль каналов повторяется последовательно, и результаты контроля оперативно отображаются на дисплее.

Технические характеристики:

Дальность обнаружения в зависимости от типа диктофона	от 0,5 до 1,5 м
Число каналов	4, 8, 16
Время обнаружения	не более 30 секунд на канал

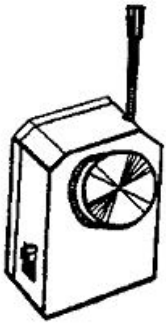
Стетоскопы. Стетоскоп представляет собой вибродатчик, усилитель и головные телефоны.

Вибродатчик специальной мастикой прикрепляется к стене, потолку и т. п. Размеры датчика, на примере устройства БТ1, составляют 2,2 × 0,8 см, диапазон частот — 300–3000 Гц, вес — 126 г, коэффициент усиления — 20 000.

С помощью подобных устройств можно осуществлять прослушивание разговора через стены толщиной до 1 м. Стетоскоп может оснащаться проводным, радио или другим каналом передачи информации. Основным преимуществом стетоскопа

можно считать трудность обнаружения, т. к. он может устанавливаться в соседних помещениях.

В качестве примера приведем два устройства — 51PE K5 и 51PE OPTO2000, отличающиеся каналом передачи. Микрофон-стетоскоп размером 2 × 3 см обеспечивает прослушивание через стены толщиной до 50 см и оконные рамы с двойными стеклами. Мощность передатчика 51PE K3 — 20 мВт, дальность — 250 м. Размеры передатчика составляют 44 × 32 × 14 мм, масса — 41 г, время непрерывной работы — 90 часов. ИК система 51PE OPTO 2000 обеспечивает радиус действия 500 м и имеет широкую диаграмму направленности.



Существуют стетоскопы, в которых чувствительный элемент, усилитель и радиопередатчик объединены в одном корпусе. Имеющий очень небольшие габариты, радиостетоскоп достаточно прикрепить с помощью специальной липкой массы к стене, полу или потолку в соседнем помещении. В качестве примера такого стетоскопа на рисунке изображен ***стетоскоп АД-50.***

Этот компактный стетоскоп позволяет не только прослушивать разговоры через стены, оконные рамы, двери, но и передавать информацию по радиоканалу. Имеет высокую чувствительность и обеспечивает хорошую разборчивость речевого сигнала. Рабочая частота составляет 470 МГц. Дальность передачи — до 100 м. Время непрерывной работы — 24 ч, размеры — 40 × 23 мм.

Тема 8. ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ ОСОБЕННОСТИ ПОСТРОЕНИЯ И ЭКСПЛУАТАЦИИ КАНАЛОВ СВЯЗИ

Связь является неотъемлемой частью производственной и социальной инфраструктуры Российской Федерации и функционирует на ее территории как взаимоувязанный производственно-хозяйственный комплекс, предназначенный для удовлетворения нужд граждан, органов государственной власти (управления), обороны, безопасности, охраны правопорядка в Российской Федерации, физических и юридических лиц в услугах электрической и почтовой связи.

Средства связи вместе со средствами вычислительной техники составляют техническую базу обеспечения процесса сбора, обработки, накопления и распространения информации.

§ 1. Понятие и назначение систем связи

Развитие и обеспечение устойчивой и качественной работы системы связи являются важнейшими условиями практической деятельности ОВД, которая немыслима без интенсивного обмена информацией самого разного характера и вида представления.

Несмотря на качественный скачок в развитии разнообразных средств связи, появившийся выбор в отношении технических систем и средств передачи информации, существуют базовые определения, не зависимые от конкретной реализации отдельных видов связи, определенные в законе «О связи». К ним относятся следующие понятия:

– абонент — пользователь услугами связи, лицо, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации;

– линейно-кабельные сооружения — сооружения электросвязи и иные объекты инженерной инфраструктуры, созданные или приспособленные для размещения кабелей связи;

– пользовательское оборудование (оконечное оборудование) — технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей;

– оператор связи — юридическое лицо или физическое лицо, оказывающие услуги связи на основании соответствующей лицензии;

– сеть связи — технологическая система, включающая в себя средства и линии связи, предназначенные для организации электросвязи;

– средства связи — технические средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи;

– электрическая связь (электросвязь) — всякая передача или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам;

– сети электросвязи — технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания;

– единая сеть электросвязи (ЕСЭ) — комплекс технологически сопряженных сетей электросвязи на территории Российской Федерации, обеспеченный общим централизованным управлением;

– сеть связи общего пользования — составная часть взаимоувязанной сети связи Российской Федерации, открытая для пользования всем физическим и юридическим лицам, в услугах которой этим лицам не может быть отказано;

– ведомственные сети связи — сети электросвязи министерств и иных федеральных органов исполнительной власти, создаваемые для удовлетворения производственных и специальных нужд, имеющие выход на сеть связи общего пользования;

– технологические сети связи — сети электросвязи федеральных органов исполнительной власти, а также предприятий, учреждений и организаций, создаваемые для управления внутрипроизводственной деятельностью и технологическими процессами, не имеющие выхода на сеть связи общего пользования;

– выделенные сети связи — сети электросвязи физических и юридических лиц, не имеющие выхода на сеть связи общего пользования.

Связь в Российской Федерации основана на комплексе технологически сопряженных сетей связи общего пользования и ведомственных сетей электросвязи на территории Российской Федерации. Она обеспечена общим централизованным управлением, независимо от ведомственной принадлежности и форм собственности.

Сеть связи общего пользования предназначена для предоставления услуг связи на территории Российской Федерации и включает в себя все сети электросвязи, находящиеся под юрисдикцией Российской Федерации, кроме выделенных и ведомственных сетей связи, независимо от их принадлежности и форм собственности.

При построении и оборудовании сети связи общего пользования учитываются требования обеспечения надежности указанной сети при воздействии на нее дестабилизирующих факторов.

Ведомственные сети связи создаются и функционируют для обеспечения производственных и специальных нужд федеральных органов исполнительной власти, находятся в их ведении и эксплуатируются ими. Ведомственная связь для нужд обороны, безопасности и охраны правопорядка в Российской Федерации обеспечивается органами связи соответствующих федеральных органов исполнительной власти. Сопряжение ведомственных сетей связи с сетью связи общего пользования производится на основе обеспечения соответствия технических средств и сооружений связи ведомственных сетей связи требованиям и техническим нормам, установленным для сети связи общего пользования. При сопряжении выделенных сетей связи с сетью связи общего пользования указанные сети переходят в категорию сети связи общего пользования.

Организационно-техническое единство системы различных государственных и ведомственных сетей достигается максимальным использованием единых средств связи и созданием сети каналов передачи информации с параметрами, принятыми для ЕСЭ. Для обеспечения этого в состав ЕСЭ входит *первичная сеть* типовых каналов передачи, типовых групповых трактов и *вторичных сетей* (рис. 8.1.1).

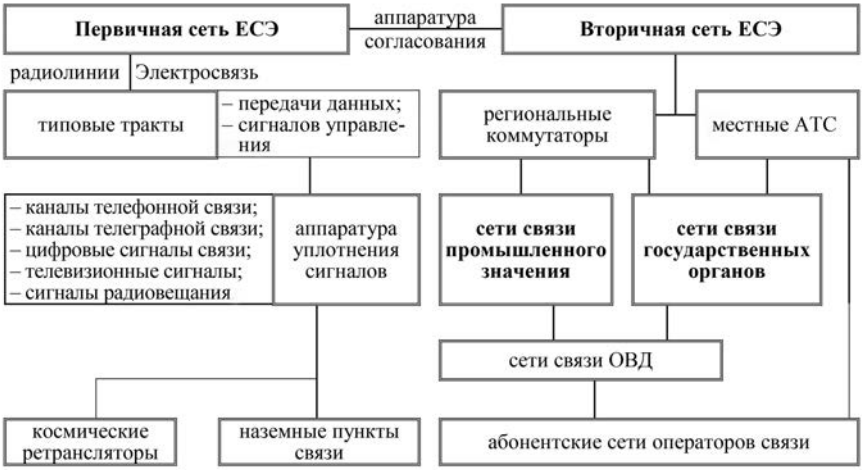


Рисунок 8.1.1 — Структура и состав ЕСЭ РФ

Первичная сеть предназначена для образования каналов и трактов передачи информации, поступающей из вторичных цепей. Она включает в себя систему воздушных и кабельных линий связи, наземные системы радиосвязи и сооружения для размещения названных устройств.

Вторичная сеть служит для непосредственного обслуживания абонентов. Она обеспечивает образование, переключение и соединение каналов связи. Вторичная сеть представляет собой совокупность средств передачи сообщений, закрепленных за потребителем, устройства коммутации, оконечные аппараты и источники питания.

Для соблюдения требований ЕСЭ при эксплуатации ведомственных средств связи органов внутренних дел (ОВД) существует приказ № 094 «Об утверждении наставления по организации связи органов внутренних дел Российской Федерации». Он комплексно регламентирует вопросы организации связи ОВД, порядок использования средств связи в служебной деятельности. Он устанавливает способы эффективного обеспечения процесса обмена информацией в ОВД, перечень технических средств связи, а также порядок, правила приема и передачи информации.

Основной задачей связи в ОВД является обеспечение четкой и бесперебойной передачи сообщений в целях непрерывного управления ОВД в любых условиях оперативной обстановки. Она обеспечивается: постоянной готовностью систем и средств связи к применению; правильным выбором способов организации связи; передачей (приемом) сообщений в установленные для оперативной информации сроки; скрытностью, конфиденциальностью, целостностью и доступностью информации легальным пользователям.

Система связи ОВД — это организационно-техническое объединение средств связи, предназначенных для обмена всеми видами документальной и речевой информации, обеспечивающее эффективное управление органами.

Система связи ОВД включает в себя узлы связи МВД РФ, управлений и отделов внутренних дел, подчиненных ОВД, объединенных общегосударственными

и ведомственными каналами в сети телефонной, телеграфной и радиосвязи. Система связи строится на базе *узлов связи* и является общей для всех служб и подразделений.

Узел связи — это организационно-техническое объединение сил и средств связи для образования переключения и коммутации каналов, обмена сообщениями в сетях связи и установления сопряжения сетей связи между собой.

В состав типового узла связи входят:

- автоматическая телефонная станция (коммутатор);
- телеграфная станция;
- пульт абонентской связи;
- радиорелейные станции и радиостанции выделенных диапазонов частот;
- аппаратура оповещения личного состава;
- аппаратура для радио- и радиотехнического контроля;
- средства магнитной звукозаписи;
- линейно-кабельные сооружения;
- устройства электропитания;
- узел связи;
- аппарат «центральная батарея»;
- телефонный коммутатор;
- однонаправленный ретранслятор;
- двунаправленный ретранслятор;
- радиорелейная станция;
- носимая радиостанция;
- портативная радиостанция;
- аппаратура магнитной записи;
- стационарная радиостанция;
- стационарная радиостанция с дистанционным управлением;
- автомобильная радиостанция.

Для организации сетей связи ОВД используются каналы и средства связи, относящиеся как к первичной, так и вторичной сетям ЕСЭ. Ведомственные сети и средства связи МВД РФ, сопрягаемые с сетями ЕСЭ, являются дополнением единой автоматизированной системы связи, организованным в интересах ОВД.

От качества и состояния системы связи напрямую зависят задачи эффективного управления силами и средствами, что налагает к системам связи определенные требования, важнейшими из которых являются:

- своевременность;
- надежность;
- достоверность;
- высокая пропускная способность;
- скрытность.

Своевременность — это способность связи обеспечивать передачу (прием) сообщений в сроки, обусловленные оперативной обстановкой.

Своевременность достигается:

- постоянной готовностью средств связи к применению;
- правильным выбором способов организации связи;
- высокой скоростью передачи(приема) сообщений;
- обученностью абонентов связи;
- обязательным выполнением правил эксплуатации средств связи;
- четким соблюдением дисциплины связи.

Надежность — это способность средств связи обеспечивать непрерывное управление деятельностью органа.

Надежность достигается:

– применением средств связи, отвечающих требованиям системы управления силами и средствами ОВД;

– наличием резерва средств и каналов связи;

– защитой каналов связи от помех;

– использованием средств связи в соответствии с их назначением.

Достоверность — это способность связи обеспечивать прием сообщений с высокой степенью точности воспроизведения передаваемой информации в пунктах приема.

Достоверность достигается:

– поддержанием эксплуатационных норм технических и эксплуатационных параметров;

– высокими практическими навыками личного состава;

– независимым дублированием каналов связи при передаче важных сообщений.

Пропускная способность — это способность связи обеспечивать своевременную передачу требуемых потоков информации.

Высокая пропускная способность достигается:

– эффективным применением средств связи;

– своевременной передачей информации на узлах связи и в подразделениях ОВД;

– сокращением массивов передаваемой информации за счет применения аппаратуры аналогово-цифрового преобразования и кодирования сигналов.

Скрытность — это способность ограничения несанкционированного доступа к схемам организации связи, передаваемой информации и аппаратуре связи.

Скрытность достигается:

– выполнением требований скрытого управления при выборе каналов и аппаратуры связи;

– строгим выполнением правил ведения переговоров по открытым каналам связи;

– оправданным применением аппаратуры маскирования речи;

– проведением мероприятий по пресечению несанкционированного доступа к средствам связи;

– соблюдением правил передачи информации по радиообмену;

– маскировкой местонахождения средств оперативной связи;

– применением аппаратуры противодействия технической разведке.

Контроль за соответствием системы связи перечисленным требованиям является важнейшей обязанностью начальника ОВД. Он обязан организовать связь в соответствии с распоряжением вышестоящего начальника с учетом имеющихся сил и средств, создавать резерв сил и средств, при необходимости принимать меры к восстановлению связи в своем подразделении. Начальник ОВД осуществляет общее руководство связью и несет ответственность за постоянную готовность средств связи к применению.

Для поддержания системы связи в постоянной готовности начальник подразделения внутренних дел обязан:

– знать оснащенность подразделения средствами связи, развивать и совершенствовать систему связи в соответствии с текущими и перспективными планами развития системы связи;

– обеспечивать правильное применение средств связи;
– организовывать работу инженерно-технического состава по их развитию;
– принимать незамедлительные меры для поддержания или восстановления связи в экстремальных условиях и при введении в действие оперативных планов.

При введении оперативных планов начальник органа имеет право наложить *ограничения на режимы работы* отдельных средств связи.

К числу таких ограничений относятся:
– запрещение работы отдельных направлений радиорелейной или высокочастотной связи;
– запрещение работы отдельных радиосетей;
– запрещение работы радиосредств на определенных частотах;
– отключение абонентов ведомственных сетей от телефонного и телеграфного канала связи.

§ 2. Виды связи

Технические средства, обеспечивающие прием и передачу информации, подразделяются на виды связи. Принадлежность средства связи к тому или иному виду определяется по среде распространения и форме представления информации. По этим признакам средства связи подразделяются на средства проводной и беспроводной связи.

Системы проводной связи предназначены для приема и передачи электрических сигналов по проводным линиям связи. Состав и назначение проводных систем связи зависят от вида передаваемых сигналов связи. По этому признаку различают аналоговые и цифровые каналы связи.

В беспроводных каналах передача информации осуществляется на основе распространения электромагнитных колебаний различных диапазонов частот, используемых в беспроводных каналах связи. Система связи, использующая в качестве носителя сообщений электромагнитные колебания радиочастотного диапазона, получила название радиосвязи.

Радиосвязью называют род электрической связи, осуществляемой между двумя или несколькими пунктами путем излучения и приема радиостанциями электромагнитных волн.

Радиосвязь в ОВД является основным видом связи, она осуществляется путем организации сетей радиосвязи различного уровня и назначения.

Сеть радиосвязи — это сеть, в которой в качестве технических средств связи используются радиостанции (или приемники и передатчики), ретрансляторы, пультовое оборудование и линии связи, сопрягающие ретрансляторы с периферийной аппаратурой радиосвязи.

При построении сетей радиосвязи ОВД в основном используются простейшие радиальные и цепочечные радиосети. Примером радиальной сети является традиционная для ОВД радиосеть одночастотного симплекса, которая позволяет осуществить связь абонентов «каждого с каждым». Примером цепочечной сети может служить сеть с цепочкой взаимосвязанных ретрансляторов или сеть радиорелейной связи.

По условиям эксплуатации, на которые рассчитаны средства связи, они подразделяются на стационарные и подвижные. По способу контроля и управления аппа-

ратурой средства связи могут исполняться как с дистанционным управлением, так и без него.

К стационарным средствам связи относятся базовые, центральные радиостанции и также ретрансляторы.

К подвижным средствам связи относятся всевозможные носимые, возимые и портативные (скрытоносимые) радиостанции и радиоприемники персонального вызова.

Современные подвижные средства связи по способу организации каналов связи включают:

- системы радиотелефонной связи;
- системы телеграфной радиосвязи;
- радиорелейные системы связи;
- транковые системы;
- пейджинговые системы;
- сотовые системы;
- спутниковые системы связи.

Системы радиосвязи используют для установления связи заранее определенный частотный канал.

Транковые системы в качестве канала связи используют принцип выбора свободного канала связи.

Пейджинговые системы используют различные виды передачи дискретных сообщений.

Сотовые системы связи используют для образования канала связи пару (для передачи и приема) выделенных каналов связи ближайшего приемопередатчика сотовой ячейки.

Спутниковые системы используют в качестве ретрансляторов сигналов космические спутники связи.

В дополнение к общей классификации сети радиосвязи подразделяются на следующие виды:

- по количеству частотных каналов — на одночастотные и многочастотные;
- по режимам работы радиосредств — на симплексные и дуплексные.

При симплексном радиообмене работающие между собой радиостанции прием и передачу сигналов ведут по очереди на одной или разных частотах.

При дуплексном радиообмене обмен сигналами связи осуществляется одновременно на разных частотах приема и передачи.

Радиорелейной связью называют род электрической связи, основанной на ретрансляции (переизлучении) радиосигналов, распространяющихся в зоне прямой геометрической видимости, с целью увеличения дальности связи.

Радиорелейная связь используется для передачи телеграфных, телефонных, факсимильных сообщений и телевизионных сигналов. Она создается путем организации радиорелейных сетей.

Сеть радиорелейной связи — это сеть, в которой в качестве технических средств связи используются радиорелейные станции, каналы радиорелейной связи, а также линии связи для сопряжения с оконечной аппаратурой радио- или проводной связи.

Радиорелейная сеть является основой первичной сети ЕСЭ, которая позволяет обеспечить высококачественную дуплексную многоканальную связь, качество которой мало зависит от времени года, суток, промышленных и атмосферных помех.

В зависимости от места в первичной сети ЕСЭ радиорелейные линии подразделяют на:

- местные (соединяют две АТС в пределах города, района);

– зоновые (внутриобластные линии связи);
– магистральные (линии передачи между зоновыми сетями);
– технологические (линии связи при обслуживании трубопроводов, железных дорог и т. д.).

Современные радиорелейные станции работают в различных диапазонах частот от 0,1 до 15 ГГц. По способу обработки информации радиорелейные станции подразделяются на аналоговые и цифровые.

В наибольшей степени требованиям надежности, достоверности и скрытности информации отвечает проводная связь.

Проводной связью называют род электрической связи, основанной на распространении электрических сигналов по проводной линии связи. К средствам проводной связи относят аппаратуру телеграфной, телефонной, факсимильной и модемной связи.

Сети телеграфной связи предназначены для передачи документированных сообщений в виде телеграмм и криптограмм. Сеть телеграфной связи в ОВД создается на базе собственных телеграфных каналов, арендованных телеграфных каналов связи ЕСЭ или каналов связи министерств и ведомств по договору.

Сети телефонной связи предназначены для обеспечения обмена информацией в виде телефонных сообщений. Телефонная связь в ОВД подразделяется на оперативную и административно-хозяйственную. Оперативная телефонная связь включает сети открытой и засекреченной телефонной связи.

Сеть засекреченной телефонной связи предназначена для ведения должностными лицами секретных переговоров по управлению ОВД. Она создается на базе каналов связи и оконечных телефонных аппаратов с использованием аппаратуры засекречивания.

Сеть открытой незасекреченной телефонной связи предназначена для ведения должностными лицами несекретных переговоров. Она создается на базе автоматических телефонных станций, коммутаторов, незащищенных линий связи и оконечных аппаратов.

§ 3. Организация и эксплуатация служебных сетей связи органов внутренних дел

В соответствии с принятой структурой управления силами и средствами в интересах оперативно-служебной деятельности создаются различные схемы организации связи.

Система связи городского (районного) ОВД представляет собой комплекс взаимосвязанных телефонных (ТЛФ), телеграфных (ТЛГ) и радиосетей. В телефонную сеть входит:

– прямая телефонная связь (выделенная линия) с вышестоящими органами;
– автоматическая телефонная междугородняя связь Министерства связи Российской Федерации;
– прямая связь с отделениями полиции, дежурными частями, подразделениями ГИБДД;
– собственная и местные ТЛФ-связи;
– спецлинии 02.

Связь с мобильными и удаленными объектами организуется с помощью сетей радиосвязи. В состав сети радиосвязи входит ВЧ-связь с вышестоящими органами и ОВЧ-связь с подразделениями.

Для обмена документальной информацией в систему связи городского (районного) ОВД входит сеть абонентской телеграфной связи Министерства связи Российской Федерации и собственная (ведомственная) телеграфная связь на обслуживаемой территории.

Для организации телефонной связи в интересах уголовного розыска и подразделений экономической безопасности и противодействия коррупции (ЭБ и ПК) используются абонентские номера городских или ведомственных телефонных сетей связи в соответствии с установленными нормами.

При наличии дежурной части в этих службах связь организуется по принципу организации связи городского (районного) отдела внутренних дел с обязательной установкой прямой связи с дежурной частью ОВД, в составе которого находится аппарат уголовного розыска и подразделений ЭБ и ПК.

Для организации связи с подвижными объектами и оперативными группами создаются отдельные или совмещенные радиосети этих служб, исходя из структуры управления и решаемых задач.

Предусматривается также создание локальных радиосетей для проведения оперативных мероприятий. Специальные электронные технические средства, применяемые в деятельности аппаратов уголовного розыска, ЭБ и ПК, при совместной работе со средствами связи не должны влиять на качественные показатели сетей связи, сопрягаемых с ЕСЭ, ведомственными сетями.

При проведении оперативно-розыскных мероприятий организуется оперативный штаб руководства, который поддерживает связь и осуществляет руководство посредством организации:

- ОВЧ-радиосетей связи с оперативными группами;
- отдельной радиосети ОВЧ-связи с группой захвата;
- ВЧ- и ОВЧ-радиосетей связи с войсковыми нарядами;
- ТЛФ-, ТЛГ-, ВЧ- и ОВЧ-связей с дежурной частью ОВД.

Организация связи оперативного штаба управления, как правило, организуется с помощью подвижного пункта связи. Количество радиосетей определяется исходя из масштаба операции, задействованных сил и средств. Управление действиями группы захвата осуществляется на отдельном радиоканале.

При введении в действие оперативных планов связь организуется в соответствии с распоряжением по связи для каждого данного плана. В ходе проведения мероприятий по оперативному плану в зависимости от складывающейся оперативной обстановки схема организации связи может видоизменяться и дополняться видами и средствами связи.

Для каждого оперативного плана должны разрабатываться справочники телефонов абонентов, радиоданные и позывные, перечень формализованных команд скрытого управления.

Правила установления телефонной связи

При ведении телефонных переговоров абоненты должны соблюдать правила, исключающие возможность разглашения государственной и служебной тайны.

Использование междугородной телефонной сети Министерства связи Российской Федерации для обмена информацией между ОВД и их подразделениями в зависимости от оперативной необходимости должно обеспечивать, в случае необходимости, возможность использования аппаратуры засекречивания.

Правила установления телеграфной связи

Телеграфная сеть ОВД предоставляет абонентам возможность круглосуточно осуществлять обмен документированной информации путем передачи телеграмм

и криптограмм. При отсутствии обслуживающего персонала подтверждение о приеме телеграмм осуществляется автоответчиком.

Аппараты телеграфной связи должны быть включены круглосуточно. Для своевременного приема информации предусматривается акустическая или световая сигнализация.

Учет исходящих и входящих телеграмм и криптограмм осуществляется в журналах установленной формы. Правила установления ТЛГ-связи определяются «Инструкцией о порядке установления соединений и обработке сообщений на ТЛГ-пунктах ОВД, включенных в сеть абонентского телеграфирования Министерства связи Российской Федерации».

По телеграфной связи запрещается передавать сообщения, в тексте которых имеются сведения секретного характера. Ответственность за утечку такой информации несет исполнитель.

Правила установления радиотелефонной связи

Радиообмен должен быть кратким, содержать минимальное количество слов и фраз.

Оценка качества радиосвязи определяется по пятибалльной системе:

- отличная связь, помехи не прослушиваются;
- хорошая связь, прослушиваются помехи;
- удовлетворительная связь, сильные помехи;
- неудовлетворительная связь;
- связь невозможна.

Переговоры на радиостанции в телефонном режиме могут проводиться непосредственно с радиостанции либо дистанционно через выносные устройства. Предоставление радиопереговоров предупреждается оператором радиостанции: «Говорите по радио».

Выходя на связь, необходимо убедиться, что канал не занят другим корреспондентом, так как вмешиваться в радиообмен разрешается только главной радиостанции (дежурная часть и далее по подчиненности).

При объявлении главной радиостанцией режима радиомолчания все корреспонденты сети должны перейти в приемный режим, при этом выход в режим передачи сигналов разрешается только в экстренных случаях (стихийное бедствие, массовые беспорядки, угроза жизни людей и т. д.)

Порядок установления радиотелефонной связи:

1. Прослушать, свободен ли канал в выбранной сети.

2. Переключиться на передачу, осуществить вызов требуемого абонента, например: «АЛЬФА», Я — «БЕТТА» *(два раза)*; Я — «БЕТТА», ПРИЕМ.

3. Для подтверждения приема сигнала вызываемая радиостанция отвечает: «БЕТТА», Я — «АЛЬФА», СЛЫШУ ХОРОШО — ПРИЕМ.

После установления связи при отсутствии передачи сообщений радиостанция переключается на прием или с разрешения главной радиостанции выключается на определенное время.

При передаче важного сообщения, а также при плохой слышимости или наличии помех подтверждение о приеме дается словами: «ПОНЯЛ ВАС», — и повторяется полный текст переданного сообщения. Об окончании работы абонент уведомляет словами: «СВЯЗЬ КОНЧАЮ».

Вмешиваться в работу между двумя станциями разрешается только главным радиостанциям, остальные радиостанции могут вмешиваться в радиообмен только при чрезвычайных обстоятельствах.

При хорошо налаженной связи и отсутствии помех, особенно на радиостанциях с фиксированной настройкой, разрешается вести телефонный обмен без применения позывных, однако перед тем, как закончить связь, передача своего позывного обязательна.

В условиях плохой слышимости трудноразличимые слова передаются по буквам, причем каждая буква передается словом, начинающимся на эту букву.

Передача сигналов осуществляется следующим образом: вызывается позывной вызываемой станции — три раза; называется свой позывной — два раза; передается «сигнал» — два раза.

Например: «АЛЬФА», «АЛЬФА», «АЛЬФА», Я — «БЕТТА», «БЕТТА», «ВЕТЕР», «ВЕТЕР».

Подтверждение в приеме сигнала производится по схеме: Я — «АЛЬФА», СИГНАЛ «ВЕТЕР» ПРИНЯЛ.

Для передачи циркулярного сообщения (адресованного всем абонентам сети) передается предварительный вызов по форме:

ВНИМАНИЕ ВСЕМ, Я — «ЦЕНТР», ПОДГОТОВИТЬСЯ К ПРИЕМУ *(два раза)*.

После паузы передается «*ТЕКСТ СООБЩЕНИЯ*» *(два раза)*.

При уверенной связи циркулярные сообщения передаются без предварительного оповещения. Подтверждение о приеме производится по форме обычного подтверждения, очередность определяется последовательностью передачи позывных, если передачи их не было, то подтверждение не требуется.

Категорически запрещается передавать открытым текстом сведения, не подлежащие оглашению:

– раскрывающие суть проводимых мероприятий;

– места дислокации заслонов, засад, временных контрольных пунктов полиции;

– называть учреждения внутренних дел, фамилии, звания и должностных лиц, адреса и телефоны сотрудников.

Лица, за которыми закрепляются средства радиосвязи, несут персональную ответственность за организацию радиообмена и сохранность материальной части. За нарушения режима радиообмена: радиообмен, повлекший за собой срыв мероприятий, радиообмен с употреблением нецензурной брани, за блокирование радиообмена в служебной сети радиосвязи (передача музыки в эфир, зажатая тангента микротелефонной трубки на длительный промежуток времени) — виновные привлекаются к дисциплинарной или материальной ответственности.

Систематический контроль за соблюдением дисциплины радиообмена осуществляется службой радио- и радиотехнического контроля круглосуточно.

Тема 9. ПРОВОДНЫЕ СРЕДСТВА СВЯЗИ

§ 1. Основные понятия электросвязи, виды и характеристики сигналов связи

Электросвязью называют технический способ обмена сообщениями путем приема и передачи электрических сигналов.

Сообщением называется информация, воплощенная и зафиксированная в форме изменения параметров электрического тока, соответственно сигналом связи называют процесс изменения во времени некоторого физического параметра электрического тока s(t), служащего для отображения, регистрации и передачи сообщения.

Характер изменения сигнала во времени может быть представлен графически, в виде осциллограммы, посредством таблицы, в которую вносятся значения s_i в некоторые (*i*-е) моменты времени (рис. 9.1.1).

Информативная составляющая сигнала может заключаться в таких физических параметрах, как амплитуда колебания (V_{max}), период его повторения (T), частота (F) и фаза (φ).

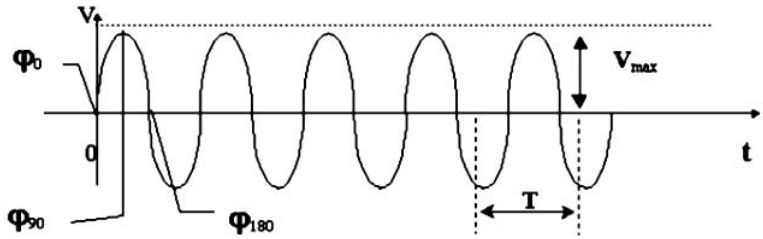


Рисунок 9.1.1 — Графическое изображение колебательного процесса

Амплитудой называется значение величины максимального отклонения колебательного процесса от среднего значения (состояния покоя).

Частотой (F) *называется количество колебаний, совершаемых за 1 секунду* (F = 1/T).

Фаза колебания (φ) *— градусная мера (от 0 до 360°), которая определяет мгновенное состояние в течение периода* (T) *совершения колебания.*

Процесс, предшествующий любым процессам осуществления электросвязи, заключается в преобразовании любого сигнала, поступающего на его вход, в соответствующее изменение электрического тока (кодировке сообщения).

Напомним, что ***электрическим током*** *называется упорядоченное (направленное) движение заряженных частиц под воздействием электрического поля. Любое изменение электрического тока в техническом устройстве, вызванное внешними воздействиями, свидетельствует о наличии информации, поэтому это изменение называется электрическим сигналом.*

Чтобы электрический ток в проводнике существовал длительное время, необходимо поддерживать в нем электрическое поле. Электрическое поле в проводни-

ках создается и может длительное время поддерживаться источниками электрического тока.

Техническое обеспечение связей между внешними и внутренними объектами связи обеспечивается организацией проводных и беспроводных (радио-, магнитных и оптических) соединений. При этом физическое взаимодействие между информационными объектами образуется на трех уровнях — среда передачи, линии и каналы связи.

Среда передачи — это материальный объект, проводящий информационный сигнал (звуковые колебания, электрический ток, радиоволны, магнитные поля или оптическое излучение).

Линия связи — совокупность технических средств, которые используются для обеспечения распространения сигналов в нужном направлении.

Длина линий связи различной природы возникновения колеблется от сотых долей миллиметра до десятков тысяч километров. В линию связи, кроме среды распространения, входят сигнал образующие устройства, коммутационные элементы, усилители и переходники, а также системы защиты линий от влияния помех распространению сигнала.

Канал связи — совокупность линий связи и оконечных блоков взаимодействия (т. е. приемное и передающее оборудование), предназначенных для обмена информационными сообщениями.

Как видно из определения, канал связи состоит из комплекта приемного и передающего оборудования (кодеров и декодеров канала связи), предназначенного для формирования сигналов связи (кодирования информации) и соответствующей линии связи. В зависимости от вида передаваемых сигналов связи различают аналоговые и цифровые каналы связи. В аналоговых каналах (Λ) для формирования (кодирования) сигналов применяют амплитудную, частотную, фазовую и квадратурно-амплитудную модуляции. В цифровых каналах (#) для передачи данных используют импульсные сигналы, группированные в самосинхронизирующиеся коды, которыми производят модуляцию (кодово-импульсную) тональных аналоговых сигналов.

По физической природе среды распространения (линий связи) различают проводные (электрические и оптические) и беспроводные (радио-, магнитные и оптические) каналы передачи сигналов.

В проводных системах связи, в зависимости от места и направления организации связей, используются линии связи различной протяженности. Условимся линии, организованные в пределах, не выходящих за границы отдельного объекта, соизмеримые с его размерами, называть цепями связи, в противном случае, когда проводные линии выходит за границы отдельных взаимодействующих устройств связи, — линиями связи.

§ 2. Виды проводных средств связи

Средства связи современных проводных систем связи соединены между собой парой проводов, именуемых абонентским шлейфом. Эта пара проводов используется и для подачи напряжения в цепь звукового сигнала телефонного аппарата при инициализации вызова, и для передачи звуковых сигналов автоматических телефонных станций (АТС) на телефонный аппарат, и для передачи собственно речи во время связи. Каждый из перечисленных сигналов помимо сугубо технологических

функций несет вполне определенную информационную нагрузку и может стать источником важной информации.

В зависимости от ее вида и назначения абонентских терминалов различают следующие виды проводной связи:

– *телеграфную связь* (где сигналы несут информацию о передаваемых символах алфавита);

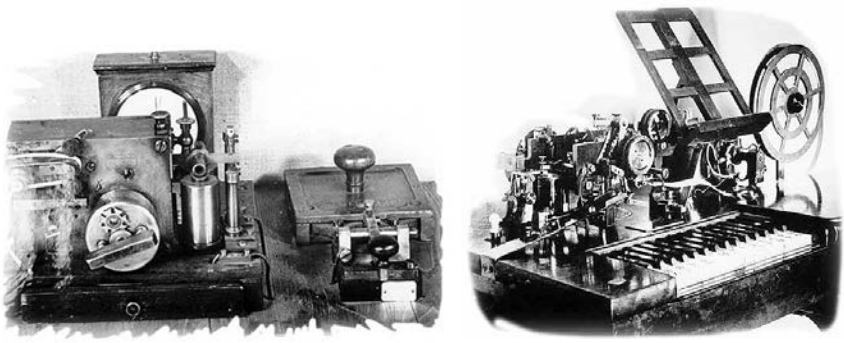
– *низкочастотную телефонную связь* (рассмотренную в предыдущем разделе);

– *факсимильную связь* (где сигналы несут информацию о пространственной и цветовой характеристике точечного (растрового) изображения);

– *модемную связь* (где сигналы предназначены для межмашинного /компьютерного/ обмена в различных сетях передачи данных).

Телеграфная связь обеспечивает передачу и прием информации в документальном виде. Здесь применяется международный телеграфный код. Сущность телеграфирования состоит в том, что каждому передаваемому знаку (букве, цифре, знаку препинания) соответствует определенная комбинация электрических сигналов. Переданная электрическая комбинация через приемные устройства приводит оба аппарата в действие, поэтому на рулонах бумаги аппаратов отпечатывается переданный знак. Передача и прием информации осуществляются с помощью специальных устройств печати, называемых телеграфными аппаратами.

Первый российский ленточный телеграф работал на основе аппаратов Морзе (1852), в последующем стали применяться буквопечатающие аппараты Юза и Казелли (рис. 9.2.1) (прообраз современного факсимильного устройства).



а) телеграфный аппарат Морзе б) телеграфный аппарат Юза

Рисунок 9.2.1 — Первые телеграфные аппараты

В начале своего развития для передачи текста требовалось вручную закодировать буквы передаваемого сообщения электрическими импульсами связи (азбука Морзе). Принцип работы современного телеграфного аппарата состоит в формировании импульсных сигналов связи, соответствующих передаваемым символам (буквам) текста, и осуществлении обратного преобразования импульсов связи в текст на приемном терминале (телеграфном аппарате).

На рисунке 9.2.2 изображен первый автоматический телеграфный аппарат (Клопфера) и операционный зал телеграфной связи.

а) телеграфный аппарат Клопфера

б) операционный зал телеграфной связи

Рисунок 9.2.2 — Телеграфные средства связи

В настоящее время применяются как ленточные, так и рулонные телеграфные печатающие аппараты типа Т-100 и ЛО-2000 с использованием приемопередающей электронной аппаратуры «Интервал», а также аппаратуры тонального телеграфирования ТТ-ЧМ-12/16 и ТТ-48. Первая передача факсимильного изображения в России была проведена в 1929 г. В это же время в стране разрабатывается и налаживается выпуск целой серии отечественных фототелеграфных аппаратов: БТОР-1, ФТ-34, 3ФТ-А4, ФТ-37, ФТ-38.

Факсимильная связь предназначена для обмена графической информацией между специальными абонентскими терминалами — телефаксами, когда требуется передача и прием полутоновых фиксированных изображений, очертаний и глубины оригинала документа.

Современный факсимильный аппарат представляет собой электромеханическое устройство, состоящее из сканера, каналообразующей аппаратуры — модема (МОдулятор-ДЕМодулятор) и принтера (рис. 9.2.3). Сканер считывает изображение документа, оцифровывает его и передает информацию в модем. Модем преобразует цифровые сигналы в последовательность модулированных сигналов и обеспечивает их передачу на другой факсимильный аппарат через обычную телефонную линию. Модем принимающего телефакса преобразует данную последовательность обратно в цифровую и передает ее на принтер. Принтер, в соответствии с полученной информацией, распечатывает изображение на бумаге.

Различают две разновидности средств факсимильной связи — автономные телефаксы, выполняющие строго определенные функции, и интегрированные системы (ИС) на базе персональных компьютеров (ПК). Первая ИС была реализована в 1985 году созданием компьютерной факсимильной платы. Сегодня компьютерные факсимильные платы выпускает огромное количество производителей. Их продукция, различающаяся по некоторым функциональным возможностям, служит одной цели — автоматизации процесса передачи, приема и распределения факсимильных сообщений, обмен которыми происходит по обычным телефонным линиям.

Кроме удобства использования, данная технология позволяет пользователям автоматизировать получение и отправку факсимильных сообщений по нескольким направлениям, что значительно повышает эффективность использования телефонных линий связи.

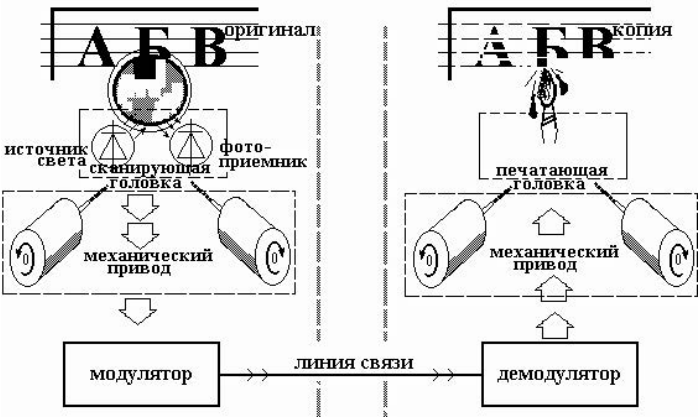


Рисунок 9.2.3 — Принцип передачи факсимильной информации

Необходимость передачи и приема цифровых данных, которые обрабатываются средствами вычислительной техники, побудила к созданию устройств, которые позволяют передавать их в проводном канале связи. Так называемые модемные технологии, как и любые технологии передачи сигналов, неразрывно связаны с характеристикой среды, по которой сигналы передаются. Учет и улучшение этих характеристик полностью определяют как характеристики, так и конструкцию современных модемов.

Процесс модуляции и демодуляции (в смысле кодирования и декодирования аналоговых сигналов) происходит следующим образом. Вначале аналоговый сигнал поступает на вход одного их каналов системы аналогово-цифрового преобразования (АЦП), где заменяется эквивалентной ему по информационному содержанию последовательностью дискретных сигналов — отсчетов.

Полоса пропускания телефонных систем ≈4000 Гц, поэтому согласно теореме Котельникова, отсчеты в каждом канале берутся с частотой $2F = 8000$ Гц. Такой процесс называется амплитудно-импульсной модуляцией (АИМ). Если максимально возможные значения сигнала на входе канала известны (или лимитированы нормами на канал), то известно максимально возможное значение отсчета. Далее каждый отсчет заменяется некоторым двоичным кодом, учитывающим знак и амплитуду отсчета. Такой процесс носит название импульсно-кодовой модуляции — ИКМ.

При передаче цифрового кода данных кодер (модема) вырабатывает соответствующую ему импульсно-кодовую (ИКМ) последовательность двоичных сигналов (при этом положительный импульс напряжения будет, например, соответствовать — «1», а отрицательный — «0»). Нетрудно подсчитать, что при 8-разрядной ИКМ скорость передачи двоичных импульсов для одиночного телефонного канала будет равна $2F \cdot 8 = 2 \cdot 4000 \cdot 8$, то есть 64 000 бит/с. При приеме последовательность принимаемых двоичных импульсов разбивается специальным методом на восьмерки (коды принятых отсчетов), которые кратковременно запоминаются и затем в параллельном виде подаются на вход цифроаналогового преобразователя (ЦАП), в котором производится преобразование цифрового кода в аналоговый сигнал. Таким образом, одному модему должен предоставляться один из цифровых каналов с временным разделением каналов с пропускной способностью до 64 Кбит/с.

Именно такую скорость передачи данных обеспечивают современные компьютерные модемы, состоящие из двух самостоятельных конструктивных частей:

– цифровой (цифровой сигнальный процессор, блок оперативной и постоянной памяти, интерфейс связи с компьютером, ISA, PSI — для внутренних и USB RS-232 — для внешних модемов);

– аналоговой (преобразователи АЦП/ЦАП и дифференциальное устройство сопряжения с аналоговой линией связи) (рис. 9.2.4).

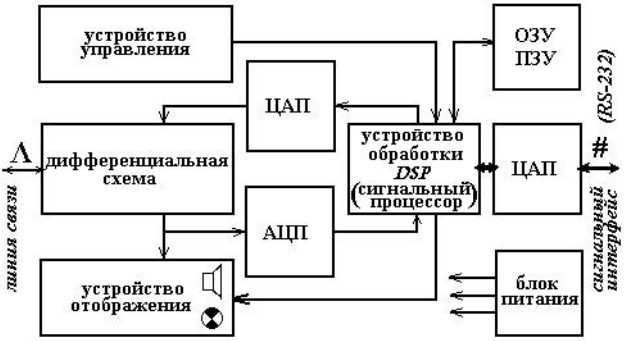


Рисунок 9.2.4 — Структурная схема модема

Такая конструкция позволяет использовать эти модемы как в роли обычных аналоговых модемов, так и в роли цифровых. Следует отметить, что скорость передачи по аналоговым линиям связи от модема клиента к цифровому модему сервера отличается от скорости приема и составляет не более 115 000 бит/с.

§ 3. Принцип работы телефонного аппарата и состав проводного канала связи

В системе проводной связи информация передается в виде электромагнитных колебаний по проводным линиям связи, которыми соединяются передатчик и приемник (аппаратура абонентов), образующие канал проводной связи. Наиболее распространенными линиями связи являются телефонные. Стандартом определена полоса пропускаемых частот телефонной линии связи, она лежит в пределах 300–3400 Гц.

В настоящее время основными проводными линиями связи являются три вида проводников:

– несимметричная пара;
– симметричная (витая) пара;
– коаксиальный кабель.

Несимметричные пары используются для абонентских соединений оконечных аппаратов к распределительным щитам телефонных сетей.

Симметричная пара (витая пара) в своей основе имеет скрученную пару медных изолированных проводов, один из которых обвит вокруг другого. Этот второй вьющийся провод предназначен для устранения взаимного влияния между соседними витыми парами. Витая пара широко используется в телефонии. Линии из

витой пары могут иметь протяженность до нескольких километров без промежуточного усиления. Она может быть использована для передачи как цифрового, так и аналогового сигналов. Пропускная способность зависит от толщины линий и расстояния, при этом достигается скорость передачи до 10 мегабит в секунду.

Коаксиальный кабель широко используется для передачи пакетов сигналов информации в компьютерных сетях, кабельном телевидении, системах видеонаблюдения и других радиотехнических комплексах. Ее основу составляет конструкция, предусматривающая такое расположение проводников, когда один из них (сигнальный) находится внутри другого, разделенные диэлектриком. Есть два основных вида коаксиальных кабелей — 50-омный (среднечастотный, для передачи цифровых сигналов) и 75-омный (широкополосный — для передачи аналоговых радиочастотных сигналов), хотя эти различия носят больше исторический характер, нежели технический.

В первичных сетях электросвязи в настоящее время успешно развивается применение и оптических кабелей с использованием одномодовых или многомодовых оптоволоконных световодов. По этому типу кабелей передаются не электрические, а оптические сигналы.

Волоконная оптика строится из волокон силикатного стекла или других подобных материалов с диаметром от 10 до 400 мкм с покрытием, имеющим несколько меньшую диэлектрическую постоянную. Волокна не обладают индуктивностью, поэтому они не подвержены действию электромагнитных помех. Такой кабель прокладывают и под землей, и под водой. Соединяют его электрически с помощью специальных коннекторов, механически, или сваривая оба конца, прижимая один край к другому.

По проводным линиям связи в зависимости от назначения и типа приемопередающих устройств организуются следующие каналы связи:

- каналы телефонной (аналоговой, цифровой) связи;
- каналы телеграфной связи;
- каналы факсимильной связи;
- каналы передачи данных.

В канал телефонной связи входят оконечные устройства, формирующие информацию, коммутационная (соединительная) аппаратура и проводные линии связи.

В качестве оконечных устройств (аппаратуры абонентов) в телефонии используются телефонные аппараты, предназначенные для приема и передачи речевой информации; в телеграфии — знакопечатающие аппараты, предназначенные для передачи и приема текстовой информации; в факсимильной связи — фототелеграфные аппараты, передающие и принимающие неподвижные изображения (фотографии, рисунки, чертежи и т. д.); в каналах передачи данных и цифровой телефонной связи — модемы (кодеки), предназначенные для преобразования импульсного цифрового кода в соответствующие ему низкочастотные тональные сигналы.

Типичным и наиболее распространенным типом аналоговых каналов связи являются телефонные каналы общего пользования (каналы тональной частоты). Канал телефонной связи образуется парой оконечных (телефонных) аппаратов, абонентскими и соединительными линиями связи, а также коммутационным оборудованием автоматической или ручной телефонной станции (коммутатором) (рис. 9.3.1).

Отметим одну важную деталь — число соединительных линий между двумя коммутационными станциями значительно меньше емкости каждой из них.

Рисунок 9.3.1 — Состав телефонного канала связи

Иными словами, соединительные линии являются групповыми элементами сети, и само коммутационное оборудование в большей своей части является групповым, т. е. им пользуются в данный момент те, кто затребовал какого-нибудь соединения. Этим и объясняется то обстоятельство, что иногда текущий вызов получит «отказ», даже если абонент, к которому мы звоним, свободен. (Такой отказ звучит иначе, чем обычное «занято» и означает — «перегрузка» (очень быстрые гудки)).

В основе работы низкочастотного телефона лежит преобразование постоянного тока источника питания в переменное напряжение, соответствующее изменению звукового давления на микрофон и приему электрических сигналов с соответствующим обратным преобразованием их в звуковые колебания подвижной диафрагмы динамика (рис. 9.3.2).

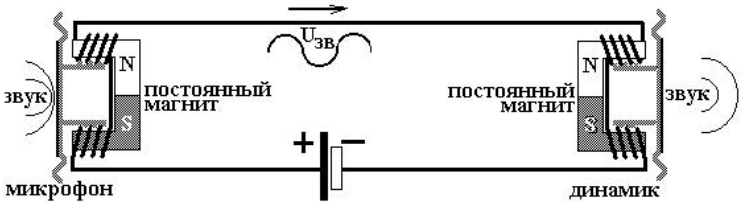


Рисунок 9.3.2 — Канал телефонной связи

Конструктивные особенности абонентских аппаратов

Абонентские аппараты телефонной связи представляют из себя оконечные точки линий проводной связи. Конструкция телефонных аппаратов предусматривает в своем составе элементы, которые обеспечивают, как минимум, выполнение следующих функций:

1) посылать запрос своей телефонной станции;

2) информировать о статусе сети (обычно это делается с помощью специальной комбинации тонов);

3) сообщать телефонной станции нужный вам номер;

4) информировать вас о поступлении вызова;

5) освобождать занимаемые ресурсы сети после завершения вызова;

6) принимать и передавать электрические сигналы связи.

Для этих целей в конструкцию телефонного аппарата (ТА) включены вызывной звонок, переключатель режима работы (занятие/освобождение линии), номеронабиратель, разговорная схема, микротелефонная схема.

На рисунке 9.3.3 показаны составные части типичного телефонного аппарата.

Рисунок 9.3.3 — Структурная схема телефонного аппарата

В отдельных случаях, например, при организации прямой (полевой или ведомственной) связи с ручной коммутацией, используют аппараты, не имеющие функций набора номера абонента.

Примером такого аппарата является полевой телефонный аппарат ТА-57. Данный аппарат обеспечивает связь до 170 км и может быть подключен в однопроводную линию связи в качестве как оконечного, так и промежуточного аппарата с питанием от местной батареи (МБ) или стационарного (центрального — ЦБ) источника питания напряжением 10 В. Батарея обеспечивает работу аппарата без замены ее в течение 3–4 месяцев.

При стандартном подключении ТА линия связи состоит из двух медных проводников, которые называются *tip* и *ring*. В соответствии с принятым соглашением жилы телефонного кабеля маркируются цветом: *tip* — зеленый провод и *ring* — красный. Конечно, в современных телефонах эти обозначения потеряли первоначальный смысл, но все еще применяются на практике.

Звонок — это устройство, предназначенное для извещения о поступившем вызове. В качестве него используются различные звуковые или визуальные извещатели, реагирующие на поступающие с оборудования телефонной станции короткие импульсы переменного сигнала с напряжением 90–120 В и частотой 20 Гц. Длительность сигналов вызова и пауз между ними определяется *звонковой каденцией,* различающейся по длительности в зависимости от характера вызова (городские и междугородние вызовы) и национального стандарта. В России звонковая каденция обычно состоит из 3 с звучания и 3 с тишины, в других странах могут использоваться другие звонковые каденции, например, в США соответствующие сигналы составляют 2–4 с, а в Великобритании 1–2 с. Звуковые извещатели, применяемые в современных ТА, подразделяются на два типа — электромеханические и электронные.

Электромеханические звонки содержат в своем составе электромагнитную систему, подвижный якорь и металлические резонаторы. Электромагнитная система имеет достаточную индуктивность и подключается к абонентской линии через конденсатор, исключающий прохождение через нее постоянного тока питания линии.

Электронные звонки, как правило, выполняются на основе пьезоэлектрического излучателя, управляемого специальной (звонковой) микросхемой.

Рычажный переключатель — это коммутационное устройство, предназначенное для переключения (в режиме разговора) линии связи с звонковой схемы на разговорную. Различают механические, релейные и электронные переключатели.

Номеронабиратель предназначен для формирования импульсных (Pulse) или тональных (Tone) адресных сигналов вызываемого абонента.

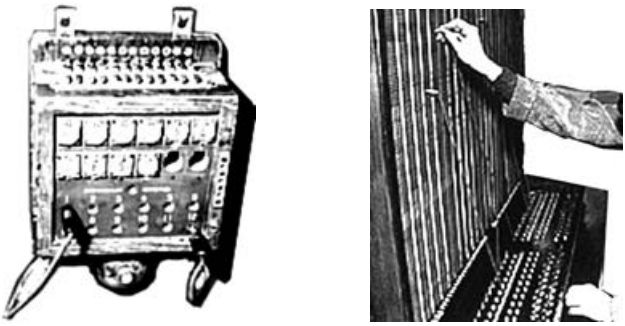
Импульсные сигналы вырабатываются механическими или электронными схемами, обеспечивающими выработку последовательностей импульсов, модулирующих постоянное напряжение питания линии связи. Физически процесс заключается в пе-

риодическом замыкании проводников линии связи. Количество закорачивающих импульсов зависит от номера набираемого абонента. Пауза между каждой группой импульсов сообщает телефонной станции о переходе к следующей цифре набора.

Коммутаторы телефонной связи

Для выбора и соединения телефонных абонентских аппаратов между собой применяются коммутационные станции ручного и автоматического обслуживания вызовов.

Начиная с 1879 года (со времени создания первого коммутатора) коммутация небольшого количества абонентов проводится телефонными станциями ручного обслуживания (рис. 9.3.4).



а) б)

Рисунок 9.3.4 — Ручные телефонные коммутаторы:
а) ручной телефонный коммутатор на 6 абонентов;
б) коммутационная стойка ручного коммутатора

В настоящее время подобные коммутаторы применяются при прокладке временных (полевых) сетей телефонной связи небольшой емкости, примером коммутатора для организации полевой телефонной связи является телефонный коммутатор П-193 с индукторным вызовом емкостью 10 абонентов. Питание усилителя рабочего места оператора осуществляется от источника питания напряжением 10 В. Дальность соединения по полевым двухпроводным линиям связи достигает 20 км.

Процесс ручной коммутации абонентов достаточно очевиден. Для уяснения процессов, происходящих при автоматическом соединении абонентов, остановимся на процессе установления одиночного соединения, в котором участвуют вызывающий (А) и вызываемый (В) абоненты.

Пока соединение не осуществлено, абонентский терминал пребывает в некотором исходном состоянии. Самый известный случай — это микротелефонная трубка, лежащая на рычаге обычного телефонного аппарата. На станцию со стороны АТ по абонентской линии в это время передается соответствующий сигнал.

Когда абонент А приступает к установлению соединения, он обычно уведомляет об этом станцию путем поднятия трубки. На станцию со стороны АТ передается сигнал занятия абонентской линии. Прибор на станции принимает его, после чего идет подготовка к приему сигналов набора номера.

Дело в том, что прием этих сигналов — довольно сложный процесс, осуществляемый с помощью сравнительных сложных и дорогих приборов. Вместе с тем время набора номера весьма мало, поэтому на станции нет необходимости на каждой абонентской линии иметь свой прибор приема сигналов набора номера. Достаточно после приема сигнала о занятии абонентской линии подключить к ней прибор приема набора лишь на время набора номера абонентом А, а затем освободить этот прибор для возможности подключения его к другой линии. Так вот, подготовка к приему сигналов набора номера и заключается в поиске свободного прибора и подключении его к соответствующей абонентской линии.

По завершении этой подготовки станция уведомляет абонента А о своей готовности. С этой целью к абонентской линии подключается источник соответствующего тонального сигнала. Услышав этот сигнал, абонент А набирает номер с помощью дискового или кнопочного номеронабирателя. В некоторых АТ это производится автоматически. На станции происходит прием и накопление сигналов номера вызываемого абонента. По окончании приема номера производится выбор пути соединения абонента А с абонентом В.

Если осуществляется внутристанционное соединение абонентов (когда оба абонента относятся к одной станции), то путь от абонента А до абонента В выбирается в коммутационной системе станции соответствующей коммутацией.

Если вызываемый абонент принадлежит другой станции, то соединение должно пройти на эту станцию либо непосредственно, либо через цепочку промежуточных (транзитных) станций. При этом на исходящей станции выбирается пучок соединительных линий в направлении требуемой соседней станции, а в пучке — свободная соединительная линия. В коммутационной системе станции производится коммутация абонентской линии А с выбранной соединительной линией.

Кроме того, эти станции обмениваются сигнальной информацией, в результате чего на соседнюю станцию передаются все данные, необходимые для дальнейшего продвижения соединения (при необходимости через промежуточные станции) до станции, к которой присоединен вызываемый абонент.

Заметим, что входящая станция (станция абонента В) может находиться как в том же районе города, что и исходящая станция (станция абонента А), так и в другом городе или стране.

После соединения с входящей станцией (как и при внутристанционном соединении) проверяется состояние вызываемого абонента (свободен он либо занят). Возможно также, что на станции вообще нет абонента с данным номером, либо он по каким-то причинам заблокирован, но эти ситуации здесь не рассматриваются.

Если абонент В свободен, к его абонентской линии подключаются соответствующие приборы и в его сторону передается вызывной сигнал, а в сторону абонента А — сопровождающий его тональный сигнал, называемый сигналом контроля посылки вызова.

После того, как вызываемый абонент поднимет трубку, передача обоих сигналов прекращается, двусторонний тракт от абонента А до абонента В готов к работе — начинается обмен информацией между абонентами.

Когда один из абонентов опускает трубку (т. е. возвращает свой АТ в исходное состояние), от «его» станции в сторону другой станции передаются соответствующие сигналы, а установленный ранее путь разрушается. В сторону второго абонента передается тональный сигнал «Занято», услышав который, абонент опускает трубку, и передача сигнала прекращается. Абонентская линия освобождается, т. е. возвращается в исходное состояние.

Если же вызываемый абонент занят, то в сторону вызывающего абонента подается тональный сигнал «Занято» и разъединение происходит после опускания трубки вызывающим абонентом.

Автоматические телефонные коммутаторы ТС по типам коммутационных приборов подразделяются на:

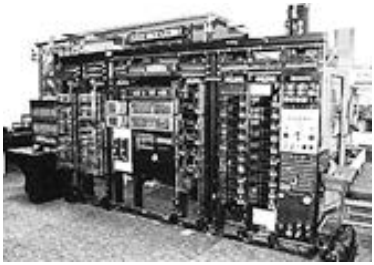
– релейные, где коммутационными приборами являются электромагнитные реле (1887 г.);

– машинные — с использованием линейных и групповых искателей линий с общим многократным полем, построенным на основе электромагнитных шаговых искателей (1900 г.);

– декадно-шаговые — на основе комбинации подъемно-вращательных, вращательных искателей и плоских телефонных реле (РПН) (1947 г.);

– механоэлектронные — на основе координатных соединителей типа Кроссбар (1954 г.) (рис. 9.3.5а);

– квазиэлектронные, в которых в качестве коммутационных приборов применены интегральные схемы и реле с герметичными контактами (герконы) (1956 г.) (рис. 9.3.5б).



а)

б)

Рисунок 10.3.5 — Автоматические телефонные коммутаторы:
а) статив механоэлектронной АТС; б) статив квазиэлектронной АТС

В настоящее время наиболее перспективными телефонными станциями являются цифровые электронные и квазиэлектронные (АТСКЭ). Их внедрение и использование является приоритетным направлением технической политики перехода единой сети электросвязи России (ЕСЭ) на систему общеканальной сигнализации 7 (ОКС7), которая предназначена для обмена сигнальной информацией в сетях связи с цифровыми программно-управляемыми станциями, которые обеспечивают работу цифровых каналов со скоростью 64 Кбит/сек., управляя установлением соединений, и может быть использована для передачи других видов информации между станциями и специализированными центрами сетей электросвязи.

Примером АТСКЭ может являться станция МТ-20/25, которая выпускается уфимским заводом коммутационной техники. Кроме основной коммутационной функции, АТСКЭ позволяет реализовать до 17 различных дополнительных видов обслуживания (ДВО):

«прямая связь» — установление соединения без набора номера вызывающего абонента;

«сокращенный набор номера» — установление соединения с использованием сокращенного набора номера (две цифры вместо пяти);

«обратный вызов» — автоматическое установление соединения к занятому вызываемому абоненту после его освобождения;

«неисправность телефонного аппарата» — автоматический вывод на станционный телетайп сообщения о номере неисправного телефонного аппарата;

«полное ограничение входящей связи» — запрет на установление входящих соединений к данному телефонному аппарату;

«наведение справки во время разговора» — установление соединения с другим (справочным) абонентом без разрушения первоначального соединения;

«злонамеренный вызов» — автоматический вызов на станционный телетайп номера вызывающего (злонамеренного) абонента;

«переадресация безусловная на другой номер» — автоматическая переадресация всех входящих вызовов к данному телефонному аппарату на другой, заданный аппарат;

«напоминание» — автоматическая выдача вызывного сигнала на телефонный аппарат в заданное время;

«постоянная переадресация при занятости» — автоматическая переадресация входящего вызова к данному телефонному аппарату в случае занятости последнего;

«ночной дежурный» — автоматическая переадресация (например, в ночное время) всех вызовов, поступающих к любому телефонному аппарату в данной группе на телефонный аппарат «дежурного»;

«уведомляющий исходящий вызов» — посылка специального сигнала уведомления занятому абоненту о поступлении к нему входящего вызова;

«передача вызова» — автоматическое установление соединения между справочным и ожидающим абонентами при отбое со стороны абонента-заказчика на ДВО «наведение справки из разговора»;

«серийное искание» — автоматическое установление соединения с одним (первым по порядку) свободным абонентом из заданной группы при наборе сокращенного номера (двух цифр 01, 02 или 03);

«сообщение об отсутствии вызванного сигнала» — автоматический вывод на станционный телетайп номера данного телефонного аппарата и сообщения об отсутствии поступления к нему вызывного сигнала;

«плохая слышимость» — автоматический вывод на станционный телетайп информации о разговорном тракте (номера ВШК или ИШК) с плохой слышимостью;

«экстренная связь» — автоматическое установление соединения к занятому абоненту.

Тема 10. СРЕДСТВА РАДИОСВЯЗИ

§ 1. Понятие радиосвязи. Основные характеристики радиосигналов

Радиосвязь является одним из основных видов связи, а во многих случаях единственным, при правильной организации и умелом использовании позволяющая обеспечить непрерывное управление ОВД в самых сложных условиях оперативной обстановки.

Под радиосвязью понимают технологии приема и передачи сигналов посредством распространения электромагнитных колебаний различных частот (в диапазоне от 0,03 до 300 ГГц) в диэлектрических средах.

Электромагнитные волны — это изменяющиеся в периодической последовательности электрические и магнитные поля, создаваемые колеблющимися с определенной частотой электрическими зарядами.

Линией радиосвязи называют совокупность среды распространения электромагнитных волн и радиотехнических устройств, обеспечивающих прием и излучение радиосигналов. Линия радиосвязи начинается с элемента, с выхода которого излучается высокочастотные сигналы связи (передающей антенны), а заканчивается элементом, на вход которого он поступает (приемной антенны).

Таким образом, линия радиосвязи образуется двумя взаимодействующими в одном частотном диапазоне антенными системами и средой распространения радиосигнала.

Важно отметить, что одна и та же линия радиосвязи может образовывать несколько одновременно действующих каналов связи, по которым передаются сигналы, отображающие различные (иногда одинаковые) сообщения, различающиеся по виду передаваемой информации, способу кодирования или несущей частоте электромагнитных волн (диапазону).

В таблице 10.1.1 перечислены виды радиосвязи, образуемые в зависимости от перечисленных особенностей сигналов в различных диапазонах.

Как видно из таблицы, особенно активно используются диапазоны НЧ, СЧ, ВЧ, ОВЧ. Радиоволны именно этих диапазонов широко применяются для передачи и приема информации, обнаружения и установления координат различных объектов (радиолокации), управления на расстоянии механизмами и устройствами определения направления на излучаемую станцию и местоположения кораблей и самолетов (радионавигации), определения места работы радиостанций (радиопеленгации).

Радиоканалы связи в подавляющем большинстве случаев организовываются в атмосфере Земли (за исключением случаев радиосвязи между подводными и космическими аппаратами, а также подземными средствами радиосвязи). Радиоканал, как правило, состоит из линии радиосвязи и двух оконечных станций, а также дополнительно может содержать несколько промежуточных приемопередающих станций — ретрансляторов. Так, например, строятся линии радиорелейных систем передачи, которые обеспечивают связь в пределах прямой видимости, что ограничивает дальность между соседними станциями до 50 км при достаточной высоте подъема и размещения антенн.

Таблица 10.1.1 — Основные направления применения радиоволн различного диапазона

Диапазон	Длины волн, м	Частоты, ГГц	Вид связи (применение)
Декаметровый (ВЧ)	100–10	> 0,03	Радиотелефония, радиовещание (КВ)
Метровый (ОВЧ)	10–1	0,03 ... 0,3	Радиотелефония, радиовещание ТВ — «*HV*», транковая связь, пейджинговые системы
Дециметровый (УВЧ)	1 ... 0,1	0,3 ... 3	Сотовая связь, ТВ — «*UHV*», спутниковая связь, системы навигации (*GPS*), вычислительные сети
Сантиметровый (СВЧ)	0,1 ... 0,01	3 ... 30	Радиорелейные линии, РК в ЛВС, спутниковая связь
Миллиметровый (КВЧ)	0,01 ... 0,001	30 ... 300	Локальные вычислительные сети
Инфракрасный (ИК)	0,001 ... $7{,}5 \cdot 10^{-7}$	$3 \cdot 10^{2}$ ... $4 \cdot 10^{5}$	Одномодовые и многомодовые оптические линии связи
Видимый свет	$(7 ... 4{,}0) \cdot 10^{-7}$	$4 \cdot 105$ ... $7{,}5 \cdot 10^{5}$	Системы световой индикации

К основным характеристикам радиоволн относятся:

– T — период колебаний (т. е. время, за которое радиоволна распространяется на расстояние, равное длине волны), то есть: $\lambda = V \cdot T = V/f$, где $f = 1/T$ — частота колебаний;

– f — частота колебаний (т. е. количество колебаний амплитуды сигнала за секунду);

– λ — длина волны (т. е. путь, пройденный со скоростью света за период T).

В вакууме и воздухе скорость распространения радиоволн равна скорости света: $V = C = 3 \cdot 10^{8}$ м/с. Подставив это значение в формулу, получим: $\lambda = 3 \cdot 10^{8}/f$.

К основным свойствам радиоволн, влияющим на их распространение, относятся:

– прямолинейность распространения радиоволн в однородной среде (однородной называют такую среду, в которой диэлектрическая и магнитная проницаемости постоянны в любом направлении);

– рассеивание энергии в окружающей среде;

– поглощение энергии электромагнитной волны (на нагревание среды);

– отражение радиоволн (на границе двух сред с различными значениями диэлектрической и магнитной проницаемости);

– преломление радиоволн (при переходе из одной среды в другую);

– рефракция (искривления траектории) радиоволн в неоднородных средах;

– дифракция (огибание препятствий) радиоволн (при длине волны, соизмеримой с препятствием);

– интерференция радиоволн (сложения амплитуд двух или более электромагнитных волн) (табл. 10.1.2).

Линии радиосвязи существенно отличаются от других каналов, например, каналов проводной связи.

Таблица 10.1.2 — Зависимость особенностей распространения радиоволн от диапазона электромагнитных колебаний

Вид радиоволн	Основные способы распространения радиоволн	Дальность связи
Мириаметровые и километровые (ОНЧ и НЧ)	Отражение от Земли и ионосферы Дифракция	Тысячи км До тысячи км
Гектометровые (СЧ)	Дифракция Преломление в ионосфере	Сотни км Тысячи км
Декаметровые (ВЧ)	Преломление в ионосфере и отражение от Земли	Тысячи км
Метровые и более короткие (ОВЧ и УВЧ)	Отражение от Земли Рассеяние в тропосфере	Десятки км Сотни км

Во-первых, она может обладать очень большим затуханием, достигающим нередко 140–160 Дб. Мощность сигнала на входе приемной части канала часто измеряется величинами порядка $10^{-10} – 10^{-14}$ Вт, в то время как для надежной работы аппаратуры, регистрирующей сигнал, требуется мощность, достигающая иногда единиц ватт и более. Это значит, что приемная аппаратура канала должна иметь коэффициент усиления по меньшей мере $10^{10} – 10^{14}$ по мощности или $10^{5} – 10^{7}$ по напряжению.

Во-вторых, затухание сигналов в линии радиосвязи оказывается переменным в широких пределах. Напряженность поля электромагнитной волны в точке приема обратно пропорциональна по меньшей мере квадрату длины пути, совершенного ею, поэтому изменение уровня сигнала на входе приемной части канала в реальном диапазоне необходимых дальностей связи достигает 100–120 Дб. Это создает свои трудности в обеспечении постоянства выходного уровня сигнала, что необходимо для нормального функционирования приемной аппаратуры.

Особенно неблагоприятными становятся условия ведения связи, когда на пути движения встречаются объекты, отражающие радиоволны, так как при этом имеет место прием нескольких интерферирующих между собой лучей, что приводит к периодическим замираниям сигнала. Наиболее тяжелые условия связи в этом смысле наблюдаются в гористой местности, в городах и крупных населенных пунктах.

В-третьих, затухание передаваемых сигналов оказывается переменным в силу изменчивости параметров земной атмосферы. Это изменение наблюдается в большей степени в диапазоне коротких волн при ведении связи отраженными от ионосферы волнами. Прежде всего в силу протекающих медленных суточных изменений степени ионизации отдельных областей атмосферы возникают суточные колебания уровня сигнала. Кроме того, прием радиоволн, отраженных от ионосферы, сопровождается частыми и довольно быстрыми замираниями сигналов, вызванными интерференцией (сложением) колебаний, пришедших в точку приема различными путями.

В-четвертых, диапазон частот линий радиосвязи, ограниченный только средой распространения радиоволн, является физически общим для всех существующих средств радиосвязи, радиовещания, радионавигации и т. д., поэтому общая потребность этих средств в некоторых участках диапазона превышает их физическую емкость и ведет к появлению взаимных помех при передаче сообщений, приводящих к потере какой-то части информации.

Главной причиной разделения радиоволн на диапазоны являются особенности их распространения и различия в пропускной способности (емкости) системы связи. Чем выше рабочая частота, тем больше емкость (число каналов) системы связи, но тем меньше предельные расстояния, на которых возможна прямая передача между двумя пунктами без ретрансляторов.

§ 2. Виды и особенности распространения радиоволн различных диапазонов

Классификация наиболее распространенных диапазонов электромагнитных волн (по частотным диапазонам), которые используются в беспроводных и оптических каналах связи, приведена в таблице 10.2.1.

Таблица 10.2.1 — Международная классификация диапазонов радиоволн

Аббревиатура	Название	Частота	Длина волны
ОНЧ (особонизкочастотные) СДВ (сверхдлинные)	Мириаметровые	1–3 кГц	100–10 км
НЧ (низкочастотные) ДВ (длинноволновые)	Километровые	3–30 кГц	10–1 км
СЧ (среднечастотные) СВ (средневолновые)	Гектометровые	30–3000 кГц	1000–100 м
ВЧ (высокочастотные) КВ (коротковолновые)	Декаметровые	3–30 МГц	100–10 м
ОВЧ (особовысокочастотные) УКВ (ультракоротковолновые)	Метровые	30–300 МГц	10–1 м
УВЧ (ультравысокие) УКВ (ультракоротковолновые)	Дециметровые	300–3000 МГц	100–10 см
СВЧ (сверхвысокие) УКВ (ультракоротковолновые)	Сантиметровые	3–30 ГГц	10–1 см
КВЧ (крайневысокие) УКВ (ультракоротковолновые)	Миллиметровые	30–3000 ГГц	10–1 мм
ГВЧ (гипервысокие) УКВ (ультракоротковолновые)	Децимиллиметровые	300–3000 ГГц	1–0,1 мм

Километровые и гектометровые радиоволны (НЧ- и СЧ-диапазонов) мало поглощаются при прохождении в толще суши или моря. Так, волны длиной 20–30 км могут проникать в глубину моря на несколько десятков метров и, следовательно, могут использоваться для связи с погруженными подводными лодками, а также для подземной радиосвязи. К тому же в этих диапазонах радиоволны хорошо дифрагируют вокруг сферической поверхности Земли, образуя так называемые *поверхностные* радиоволны. Оба эти фактора обусловливают возможность распространения длинных и сверхдлинных волн поверхностной волной на расстояние порядка 3000 км.

Метровые волны (ОВЧ-диапазона) длиной от 10 до 1 м могут распространяться поверхностными волнами. С повышением частоты сильно возрастает поглощение волн в полупроводящей поверхности Земли. Поэтому при обычных мощностях передатчика поверхностные волны ОВЧ-диапазона распространяются на расстояния, не превышающие нескольких десятков километров.

Пространственные радиоволны (ВЧ-диапазона) могут распространяться на многие тысячи километров путем переотражения от ионосферы и поверхности Земли, причем для организации такой связи не требуется передатчиков большой мощности. Поэтому в настоящее время для связи и вещания на большие расстояния используются главным образом радиоволны ВЧ-диапазона.

Метровые волны (ОВЧ- и УВЧ-диапазонов), которые часто называют ультракоротковолновыми волнами (УКВ), со стороны более низких частот примыкают к коротким волнам, а со стороны высоких частот граничат с длинными инфракрасными лучами.

Граница этого диапазона определена тем, что на этих волнах, как правило, не может быть удовлетворено условие отражения радиоволн от ионосферы (рис. 10.2.1).

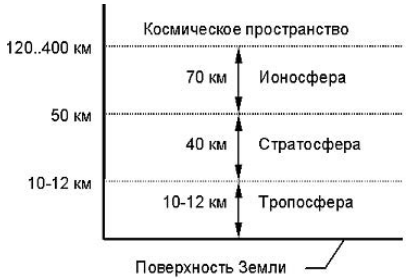


Рисунок 10.2.1 — Строение атмосферы Земли

Весь метровый диапазон разбит на четыре поддиапазона: метровый (ОВЧ — 30–300 МГц), дециметровый (УВЧ — 300–3000 МГц), сантиметровый (КВЧ — 3000–30 000 МГц) и миллиметровый (ГВЧ > 30 000 МГц). Каждый из перечисленных поддиапазонов радиоволн имеет свои особенности и находит применение в технике.

Диапазон ОВЧ-радиоволн используется в телевидении, частотно-модулированном вещании и организации связи с мобильными объектами, а в последнее время — и для осуществления радиорелейной и космической радиосвязи.

Диапазоны дециметровых и сантиметровых волн (УВЧ и КВЧ) используются в телевидении, радиолокации и многоканальной связи.

При организации дальней ОВЧ-радиосвязи применяют направленные антенны, поднятые над поверхностью Земли на значительную высоту в масштабе длины волны.

Большинство радиостанций, входящих в систему связи ОВД, работает в ОВЧ-диапазоне. Радиосвязь в данном диапазоне предназначается главным образом для оперативного управления подвижными силами ОВД. Эта связь осуществляется с помощью специально сконструированных стационарных, подвижных и носимых радиостанций, работающих в отведенных для ОВД участках ОВЧ-диапазона.

Поверхностные радиоволны ОВЧ-диапазона распространяются в пределах прямой геометрической видимости. Прямая видимость определяется видимостью антенн корреспондирующих радиостанций. Вместе с тем поверхностные

волны обладают способностью сгибать незначительные препятствия на пути своего распространения. Они отражаются от препятствий и частично проникают через них. По этой причине распространение поверхностных радиоволн (особенно в ОВЧ-диапазоне) на сильно пресеченной или интенсивно застроенной местности представляет чрезвычайно сложную картину. В связи с этим дальность практического установления связи, как правило, трудно высчитать теоретически; она устанавливается практическим путем, поэтому при практической организации связи, например, канала связи с патрульными автомашинами, в условиях большого города опытным путем устанавливают, в каких местах маршрута есть связь, в каких она отсутствует, а затем дают рекомендации патрульной группе.

Особенности средств радиосвязи в ОВЧ-диапазоне следующие:

– портативность радиостанций;
– простота управления их работой;
– возможности использования как в стационарных условиях, так и на подвижных объектах;
– обеспечение бесперебойной связи в любое время суток и года.

Радиостанции ОВЧ- и ВЧ-диапазонов обеспечивают симплексную (т. е. передача и прием информации между работающими радиостанциями происходят поочередно), беспоисковую и бесподстроечную радиосвязь на строго фиксированных частотных каналах.

К недостаткам радиосвязи ОВЧ-диапазона относят свойство прямолинейного распространения и значительного затухания (ослабления) радиоволн в атмосфере. Однако при организации ретрансляционной сети с помощью маломощных ОВЧ-радиопередатчиков в малых обслуживаемых зонах (так называемых сотах) появляется возможность организации современных сетей сотовой или транкинговой связи. Принцип сотовой организации связи заключается в многократном использовании ограниченного числа радиочастотных каналов ОВЧ-диапазона в отдаленно расположенных зонах связи, называемых сотами. Располагая последовательно группы сот, можно расширить зоны действия сотовой системы связи вширь, уменьшая мощность ретрансляционных передатчиков внутри ячеек, можно разбить ячейку на более мелкие, увеличивая количество обслуживаемых абонентов.

К наиболее распространенным средствам радиосвязи ОВЧ-диапазона ОВД относятся ***радиостанции систем «Motorola», «Сапфир», «Радий», «Алмаз»,*** а также различные системы транкинговой и сотовой связи.

При организации радиосвязи в ОВЧ-диапазоне необходимо учитывать особенности распространения поверхностных радиоволн, характер и рельеф местности, на которой организуется радиосвязь, и соответственно размещать на ней антенны стационарных радиостанций, способных обеспечить связь на заданной территории как между стационарными, так и с подвижными радиостанциями.

§ 3. Состав, принцип работы и назначение элементов радиопередающих устройств

Каналообразующие устройства, предназначенные для организации радиосвязи, представляют собой передающие и принимающие блоки, выполняющие функции формирования, излучения и приема электромагнитных колебаний, в параметрах которых заключено передаваемое сообщение. Радиопередатчик — это техническое устройство, предназначенное для преобразования передаваемых сообщений в сиг-

налы радиосвязи и излучения их в пространство. Радиоприемник предназначен для приема радиосигналов, выделения заключенного в них информационного сообщения и выдачи его в требуемой для конкретного вида связи форме.

Для обеспечения симплексной радиосвязи в пункте, из которого ведется передача сигналов, размещают радиопередающее устройство, содержащее радиопередатчик и передающую антенну, а в пункте, в котором ведется прием сигналов — радиоприемное устройство, содержащее приемную антенну и радиоприемник.

Для двухстороннего обмена сигналами нужно иметь два комплекта оборудования. Двухсторонняя радиосвязь может быть симплексной или дуплексной. При симплексной радиосвязи передача и прием ведутся поочередно. Радиопередатчики в конечных пунктах в этом случае могут работать на одинаковой частоте, на эту же частоту настроены и радиоприемники. Радиопередатчик включается только на время передачи. При дуплексной радиосвязи передача осуществляется одновременно с приемом. Для связи должны быть выделены две разные частоты для передачи в разных направлениях.

Исторически сложилось, что *радиостанцией называется комплект, состоящий из приемного и передающего оборудования, предназначенного для организации канала радиотелефонной связи (РТС).*

Система радиопередачи символов и отображения текстовой информации получила название пейджинговой системы (*page* — страница), соответственно приемник в этой системе называется *пейджер*, а приемопередатчик — *твейджер* (*two way page* — двунаправленная страница).

Системы многоканальной радиосвязи с автоматической коммутацией ограниченного количества каналов связи называются транковыми системами (*trunk* — ствол). Отличием *транковых радиостанций* является включение в их состав блока адресации вызова, аналогичного вызывной системе проводной телефонии.

В настоящее время в отдельный вид беспроводной связи выделилась сотовая связь как разновидность высокоподвижной радиосвязи, отличающаяся прежде всего массовостью обслуживания абонентов на ограниченной территории. При этом исторически сложилось так, что сотовая связь постепенно расширила сферу обслуживания телефонной сети общего пользования.

Вообще-то сам термин «сотовая связь» — это общепринятое сокращенное наименование услуги, получаемой с помощью развернутых сотовых сетей подвижной связи, выполненных на базе соответствующих систем. Таким образом, этот термин характеризует именно подвижную связь. Такие длинные рассуждения необходимы, чтобы не путать сотовую сеть и сотовую связь, ибо первая означает способ осуществления радиопокрытия определенной территории (соответственно может использоваться для предоставления услуг как подвижной, так и фиксированной связи), а вторая — услугу в виде передачи и приема информации исключительно между подвижными абонентами сотовой сети, причем сегодня это может быть не только речь, но также данные, например по технологии WAP (*Wireless Application Protocol*), то есть протоколу беспроводного доступа к сети Internet. Данный протокол (технический стандарт) представляет собой технологию, обеспечивающую пользователям мобильных телефонов простой и быстрый доступ в сеть Internet. Этот протокол оптимизирован не только для использования в канале сотовой связи, но и для отображения информации на дисплеях современных сотовых телефонов, имеющих (по сравнению с мониторами ЭВМ) ограниченные возможности.

Технология WAP позволяет сочетать телефонное обслуживание с поисковой системой и обеспечивает простой интерактивный доступ в Интернет с сотового телефона.

Типичные приложения WAP включают электронную торговлю, банковское обслуживание через Internet, получение информации и сообщений. При постепенном переходе сотовых сетей к технологиям третьего поколения, использующих пакетные технологии обмена данными — GPRS (*General Packet Radio Service*), приложения WAP станут более востребованными, так как процесс обмена данными примет более высокий темп передачи данных по сравнению с сетями GSM (до 115 200 бит в секунду).

К конструктивным отличиям сотовых телефонных (и портативных спутниковых) терминалов относятся:

– наличие блока адресации вызова;
– присутствие электронного идентификатора абонента сети;
– использование схемы автоматического поиска ретранслятора (спутника связи) сети связи.

К средствам радиосвязи можно отнести и системы автоматического определения местоположения абонента. Примером такого использования средств радиосвязи служит система GPS (*Global Position System*), которая использует радиоканалы связи со спутниками для определения географической точки стояния приемника GPS. В системе применяются либо только приемники сигналов географических координат (пассивный вариант использования) либо радиостанции, которые передают телеметрическую информацию о состоянии абонента.

Конструктивно в состав таких радиостанций дополнительно включены жидкокристаллические (ЖК) дисплеи для отображения карт местности, микропроцессорные вычислительные системы для хранения, смены и отображения местности и интерфейс связи с внешними датчиками.

Прочие особенности перечисленных средств связи будут подробнее рассмотрены в соответствующих разделах.

Структура и принцип работы средств радиосвязи

Для рассмотрения общих принципов работы радиосредств необходимо представить структуру и функциональные особенности компонентов, необходимых для их работы (рис. 10.3.1).

Для пояснения работы радиостанции воспользуемся эпюрами напряжений сигналов, которые формируются в различных составных частях радиостанции.

Порядок работы и взаимодействия составных частей следующий:

1. Источником сообщений в РТС служит микрофон, с его выхода электрический низкочастотный сигнал *A* поступает на соответствующий усилитель.

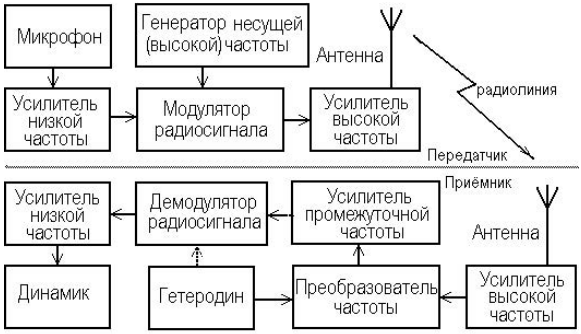


Рисунок 10.3.1 — Структурная схема радиостанции

2. После усиления сигнал поступает на вход модулятора, который предназначен для изменения одного из параметров высокочастотных колебаний *Б*, вырабатываемых генератором высокой частоты по закону изменения низкочастотного сигнала (в РТС, как правило, изменяется амплитуда, частота или фаза ВЧ-сигнала).

3. Далее промодулированный ВЧ-сигнал *В* (или в случае частотно-модулированного — *Г*) усиливается до требуемого значения.

4. После этого усиленный сигнал излучается с помощью антенного устройства в окружающее пространство.

При приеме радиотелефонный высокочастотный сигнал улавливается антенным устройством и поступает в высокочастотный усилитель, где происходит его предварительная обработка (селекция и усиление), далее, как правило, в приемном устройстве происходит понижение частоты ВЧ-сигнала на более низкую — промежуточную частоту.

Возможность настройки приемной схемы на несущую частоту радиосигнала обеспечивается узкополосным фильтром, находящемся на выходе преобразователя, который пропускает сигнал только одной, так называемой промежуточной частоты ($F_{\text{пч}}$). Таким образом, настройки радиоприемного тракта можно менять, изменяя частоту ($F_{\text{гет}}$), вырабатываемую специальным генератором — гетеродином, который, взаимодействуя с радиочастотным сигналом, принятым антенной, понижает частоту принятого сигнала до $F_{\text{пч}}$:

$$F_{\text{пч}} = F_{\text{рс}} - F_{\text{гет}}.$$

С одной стороны, это позволяет упростить настройку приемной системы, а с другой стороны, — исключить из схемы высокоточные элементы и сложные технические устройства обработки сигналов на высокой частоте.

После предварительной фильтрации принятый сигнал поступает в демодулятор, где происходит выделение низкочастотной информационной составляющей принятого сигнала. В зависимости от применяемого вида модуляции, демодулятор производит либо амплитудное детектирование (амплитудный детектор) НЧ-сигнала, либо частотную или фазовую дискриминацию (частотный дискриминатор).

После выделения информационной составляющей НЧ-сигнал усиливается до величины, необходимой для работы устройства воспроизведения звука — динамической звуковой системы.

Исходя из изученных принципов работы радиосредств, можно констатировать, что основными характеристиками радиостанций являются: чувствительность приемника, выходная мощность передатчика, диапазон рабочих частот, число фиксированных каналов связи и (соответственная) дальность установления связи.

Под чувствительностью радиоприемника понимают его способность принимать слабые по уровню сигналы от передатчиков корреспондентов и обеспечивать при этом заданный режим работы оконечного устройства (т. е. усиливать и преобразовывать принятые сигналы в звуковые колебания нормальной громкости).

Выходная мощность передатчика — это мощность, излучаемая передатчиком через антенну в пространство.

Под диапазоном рабочих частот понимается частотный диапазон, в пределах которого работает данная радиостанция.

Под дальностью радиосвязи понимается максимальное расстояние между радиостанциями в условиях прямой геометрической видимости, на котором можно осуществить устойчивую связь.

Тема 11. СРЕДСТВА СВЯЗИ С МОБИЛЬНЫМИ ОБЪЕКТАМИ

§ 1. Классификация систем радиосвязи с мобильными объектами

Напомним, что принципиальное отличие радиосистем передачи информации от проводных систем заключается в том, что условия распространения радиоволн подвержены непрерывным изменениям, зависящим от времени и частоты. Однако передача с помощью радиоволн в некоторых случаях является единственным методом организации связи (например, связь с подвижными объектами).

В ОВД применяются различные системы радиосвязи: радиотелефонные УВЧ-, ВЧ- и ОВЧ-диапазонов, радиорелейные прямой видимости и тропосферные, спутниковые, ионосферные и пр.

Для организации двухстороннего обмена сигналами в различных системах связи, как правило, предусматриваются два комплекта оборудования.

Двухсторонняя радиосвязь может быть симплексной или дуплексной. При симплексной радиосвязи передача и прием ведутся поочередно. Радиопередатчики в конечных пунктах в этом случае могут работать на одинаковой частоте, на эту же частоту настроены и радиоприемники. Радиопередатчик включается только на время передачи. При дуплексной радиосвязи передача осуществляется одновременно с приемом. Для связи должны быть выделены две разные частоты для передачи в разных направлениях. Радиопередатчики и радиоприемники абонентов включены в течение всего сеанса связи.

Для организации радиосвязи с мобильными объектами применяются:

- системы радиотелефонной связи (ВЧ- и ОВЧ-диапазоны);
- системы пакетной радиосвязи;
- транковые системы связи;
- сотовые системы связи;
- спутниковые системы связи.

Радиосвязь в ВЧ-диапазоне осуществляется, главным образом, пространственной волной на расстояниях от 100 до 1000 и более километров. При организации связи в ВЧ-диапазоне на большие расстояния необходимо учитывать географическое направление линий радиосвязи, время суток, сезон года и протяженность линии радиосвязи, так как влияние этих факторов связано с состоянием и положением слоев ионосферы над земной поверхностью. Рекомендуемые направления применения радиосредств ВЧ-диапазона представлены в таблице 11.1.1.

Такая радиосвязь обычно используется для организации региональной сети радиотелефонной связи, радиовещания и пакетной связи на направлениях, где недостаточно развиты средства проводной междугородной телефонно-телеграфной связи.

По конструкции и назначению радиостанции ВЧ-диапазона (коротковолновые радиостанции) делятся на радиотелефонные, радиотелеграфные и универсальные радиостанции, а также радиокомплексы пакетной связи.

Радиостанции радиотелефонной связи подразделяются на стационарные (типа «Ангара-1с», «Родник-22, «Полоса-2»), комбинированные (типа «Ангара-1У»), носимые (типа «Ангара-1Н2», «Карат-2Н») и универсальные /предназначенные для телефонной и телеграфной связи/ (типа Р-123, Р-123м, Р-105, Р-107).

Таблица 11.1.1 — Основные направления применения радиосредств ВЧ-диапазона

Диапазон	Оптимальное применение	Направление использования	Противопоказания	Примечание
27 МГц	Дальняя связь в сельских районах, при условии применения эффективных внешних антенн и мощных передатчиков	Связь между стационарными и подвижными объектами в условиях среднеэтажной и многоэтажной застройки	Внутриофисная связь и любая связь с использованием носимых радиостанций в городской застройке	Чрезвычайно высокая чувствительность к любым видам помех и к дальнему распространению сигналов
33–48 МГц	Дальняя связь в сельских районах, при условии применения эффективных внешних антенн и мощных передатчиков	Связь между стационарными и подвижными объектами в условиях многоэтажной застройки	Внутриофисная связь и любая связь с использованием носимых радиостанций в городской застройке	Средняя чувствительность к любым видам помех. В северных условиях способность дальнему распространению сигналов

Радиокомплексы пакетной связи содержат в своем составе, помимо радиостанции, устройства обработки пакетов данных и устройство управления. Как правило, эти функции выполняет компьютер под управлением специальной программы.

Принцип работы пакетной радиосвязи (*Pocket Radio*) напоминает работу радиостанций в режиме телеграфной связи. Информация в этом виде цифровой радиосвязи передается небольшими порциями (пакетами). После передачи каждой порции передающая станция выключается и ждет подтверждения правильности принятого пакета. Если приемная станция не приняла эту порцию или приняла неправильно, она сообщает об ошибке и передающая станция повторяет тот же самый пакет.

Каждый информационный пакет содержит до 256 символов. В системе пакетной связи принят протокол AX 25, устанавливающий для всех абонентов единые правила формирования цифровой последовательности сигналов. Скорость передачи по данному протоколу связи в ВЧ-диапазоне составляет не более 300 бод.

Для обеспечения бесперебойной работы на линиях дальней ВЧ-связи используются, как правило, приемопередатчики (трансиверы), обладающие высокой стабильностью частоты (≈20 Гц за сутки), мощностью до 200 Ватт, связанные с «почтовым ящиком», в котором автоматически записываются принятые и переданные сообщения. Запись, прием и передача сообщений, а также настройка комплекса производятся специальным компьютером.

К особенностям **средств радиосвязи в ОВЧ-диапазоне** относятся: портативность радиостанций; простота управления их работой; возможности использования как в стационарных условиях, так и на подвижных объектах; обеспечение бесперебойной связи в любое время суток и года.

К недостаткам радиосвязи ОВЧ-диапазона относят свойство прямолинейного распространения и значительного затухания (ослабления) радиоволн в атмосфере. Однако при организации ретрансляционной сети с помощью маломощных ОВЧ-радиопередатчиков в малых обслуживаемых зонах (так называемых сотах)

появляется возможность организации современных сетей сотовой или транковой связи. Принцип сотовой организации связи заключается в многократном использовании ограниченного числа радиочастотных каналов ОВЧ-диапазона в отдаленно расположенных зонах связи, называемых сотами. Располагая последовательно группы сот, можно расширить зоны действия сотовой системы связи вширь, уменьшая мощность ретрансляционных передатчиков внутри ячеек, можно разбить ячейку на более мелкие, увеличивая количество обслуживаемых абонентов.

К средствам радиосвязи ОВЧ-диапазона относятся станции радиотелефонной связи, например, систем «Сапфир», «Алтай» и т. д., а также различные системы транковой связи и средства пейджинговой связи.

Особенностью **транковых систем связи** является возможность автоматической коммутации и выбора абонентов связи.

В основе транкинга лежит принцип автоматического предоставления ограниченного количества каналов связи большому количеству абонентов. Все транковые системы можно разделить на два основных класса: системы с закрепленным каналом управления и системы с незакрепленным каналом управления, отдельно можно выделить и цифровые транковые системы.

Транковые системы с незакрепленным каналом управления (распределенным методом управления). К этому классу относятся системы, в которых на одних и тех же каналах происходит как передача служебной информации (кодов вызова, кодов радиостанций, телефонных номеров и т. д.), так и передача речевой информации.

В этих системах ни один из абонентов не может даже пытаться осуществить доступ до тех пор, пока не появится хотя бы один свободный канал. Абонентом, который после этого получит доступ, будет тот, кто первым сделает попытку. Этот метод доступа так и называется: «Первым пришел — первым обслужен». У всех абонентов равные уровни приоритета. Это главное отличие от систем с выделенным каналом управления, где используется метод, который позволяет всем абонентам пытаться получить доступ к системе, но при этом система отказывает в доступе абонентам с низким уровнем приоритета, не предоставляя им канал, и ставит их в очередь на обслуживание.

Главное преимущество распределенного метода управления состоит в том, что доступ к системе может быть выполнен по любому из свободных каналов. Каждый ретранслятор определяет, какой из каналов свободен, и передает эту информацию в потоке данных одновременно с речевым сообщением. Это означает, что каждый ретранслятор поддерживает собственный поток данных и обслуживает все обращения к своим каналам. Конфликтные ситуации предотвращаются самими абонентами. Это обеспечивает полностью параллельную обработку всех вызовов.

Дополнительным преимуществом распределенного управления является использование всех каналов для речевой связи. В системах с выделенным каналом управления этот канал обычно не может использоваться для речевой связи.

SmarTrunk II. Главным препятствием на пути использования систем в России является отсутствие сертификата Минсвязи на данный тип транковых систем. Главными достоинствами SmarTrunk II являются широкий ассортимент аппаратуры, простота переделки обычных радиостанций в транковые, неприхотливость в выборе рабочих частот.

Основным элементом системы SmarTrunk II является многоканальная базовая станция, оснащенная ретрансляторами и транковыми контроллерами. Однако основное управление в системах SmarTrunk II осуществляют абонентские радиостанции, которые сканируют (осматривают) рабочие каналы, ищут свободный канал для

связи или определяют, нет ли на одном из каналов вызывного сигнала для радиоабонента. Количество радиоканалов определяется исходя из количества абонентов в системе и планируемого трафика. В системе SmarTrunk II может быть от 2 до 16 каналов и, соответственно, система может обслуживать от 60 до 1100 абонентов.

Работа ***системы LTR*** (LTR450 и LTR800) основана на организации обмена служебными сообщениями между абонентской станцией и ретранслятором. Обмен данными осуществляется постоянно на субтональной частоте 150 Гц одновременно с передачей речевых сообщений. При этом отпадает необходимость в выделенном канале управления и поэтому для обеспечения максимальной эффективности системы все каналы могут быть использованы для передачи речевых сообщений. Если один ретранслятор выйдет из строя, остальные ретрансляторы остаются работоспособными.

Для местных вызовов (от одной портативной станции к другой) канал связи удерживается только на время передачи, т. е. время между передачами может использоваться другими абонентами, осуществляющими свои вызовы. Удержание рабочего канала в транковой системе LTR имеет место только в случае входящих телефонных вызовов.

Транковые системы с закрепленным каналом управления

К этому классу относятся транковые системы, в которых для передачи служебной информации используется отдельный канал связи. Основной особенностью систем с выделенным каналом является то, что один из радиоканалов в системе постоянно выделен для управления и контроля системы связи. Именно на этом канале передается вся служебная информация (коды вызова, индивидуальные номера радиостанций, статусные сообщения и т. д.) между базой и абонентскими радиостанциями. Остальные каналы используются для ведения речевых переговоров.

Наиболее известными представителями систем с закрепленным каналом управления являются системы протокола MPT 1327.

Транковый протокол MPT 1327 (Ministry of Post and Telecommunication) был разработан в Англии для радиосетей общего пользования в диапазоне 174–225 МГц. Впоследствии этот протокол получил широкое распространение в Европе и стал чем-то вроде стандарта для производителей транкового оборудования. MPT 1327 распространился и на другие диапазоны частот и в настоящее время транковая аппаратура MPT 1327 выпускается для диапазонов 146–174 МГц, 300–380 МГц, 400–520 МГц и даже 800 МГц.

Системы MPT 1327 обеспечивают быстрое установление связи и целый ряд дополнительных удобств, таких, как возможность передачи данных на борт мобильного объекта, построение многосотовых сетей связи, выявление и эффективное устранение нелегальных абонентов и т. д.

В исходном состоянии все абонентские радиостанции в пределах зоны действия данной базовой станции находятся на приеме на частоте управляющего канала. На этом канале система постоянно передает сообщения типа ALOHA — приглашение отвечать ей с уведомлением, сколько времени система ждет ответа абонентских станций.

Вызывающий абонент набирает на клавиатуре своей радиостанции номер нужного ему абонента и производит вызов. При этом его радиостанция посылает вызывную последовательность в ответ на очередную посылку ALOHA от базовой станции. Приняв вызов, база проверяет абонента по принципу «свой — чужой» и на том же управляющем канале вызывает второго абонента. Получив от него подтверждение о готовности к связи, база передает обеим радиостанциям команду на

перестройку на один из свободных в этот момент «разговорных» каналов связи (каналов трафика).

Обе радиостанции автоматически перестраиваются на указанный канал и начинают переговоры. При нажатии любым из абонентов клавиши «отбой» происходит автоматический возврат радиостанций в ждущий режим на управляющем канале.

В случае, когда все каналы трафика заняты, база помещает поступающие вызовы в очередь на обслуживание, обрабатывая вызовы по мере освобождения каналов.

Цифровые транковые системы

Наиболее современной системой транковой связи является система цифровой связи — TETRA (ТрансЕвропейская Транковая Радиосистема).

Она содержит основной вариант на передачу речи и данных (TETRA V + D = «*Voice and Data*»), а также специальный вариант, который поддерживает оптимальную передачу данных по пакетному радиоканалу (TETRA PDO = «*Packet Data Optimized*»). Кроме этого, в систему заложена возможность передачи данных, пейджинга и шифрования сигналов.

Это система основана на использовании шумоподобных радиосигналов с временным разделением каналов (CDMA). В системе предусмотрено четыре независимых каналов передачи на каждой несущей. Разнос между несущими составляет 25 кГц. По сравнению с аналоговой транковой радиосистемой, которая работает с разносом частот 12,5 кГц в соответствии со стандартом МРТ, это позволяет вдвое повысить эффективность использования частот одновременно со значительным повышением качества передачи речи. По сравнению с другими цифровыми стандартами связи (GSM, DECT и DAMPS) она обеспечивает вчетверо большую эффективность использования частот.

В качестве системы уплотнения каналов связи TETRA использует принцип разделения каналов по времени TDMA и предоставляет четыре независимых канала связи внутри одной пары радиолиний связи с разносом радиоканалов 25 кГц.

Скорость передачи на несущих частотах TETRA составляет 36 кбит/с. Кроме передаваемого сообщения, в передаваемые данные включается протокольная информация и коды, необходимые для защиты радиолинии абонент — базовая станция. Максимальная скорость передачи информации в абонентском канале составляет 7,2 кбит/с (в каждом /из четырех/ временном интервале).

Пейджинговые системы

Пейджинговые системы (ПС) представляют собой комплекс передачи цифровых данных, ориентированный на прием текстовых сообщений с помощью персональных приемников с буквенно-цифровым дисплеем.

Кроме того, в ПС предусмотрены такие ДВО, как персональная голосовая почта с оповещением на пейджер, переадресация вызовов, коммутация двух абонентов, отправка сообщений с телефонных аппаратов без помощи оператора, интеграция с системой телеметрии или сигнализации.

Основой ПС является пейджинговый терминал связи с радиопередающими станциями передачи сообщений. Терминал предназначен для организации связи компьютерной базы данных сообщений с операторским бюро и выдачи цифровых кодов передаваемых сообщений на передающие станции. В состав терминала входят ЭВМ, интерфейсы (порты) связи с информационно-вычислительным комплексом, средствами радиосвязи и управления, а также специальное программное обеспечение.

Для передачи пейджинговых сообщений используются радиопередающие устройства ВЧ- и ОВЧ-диапазонов, например, «NUCLEUS NT5481», «MOTOROLA–GM300»,

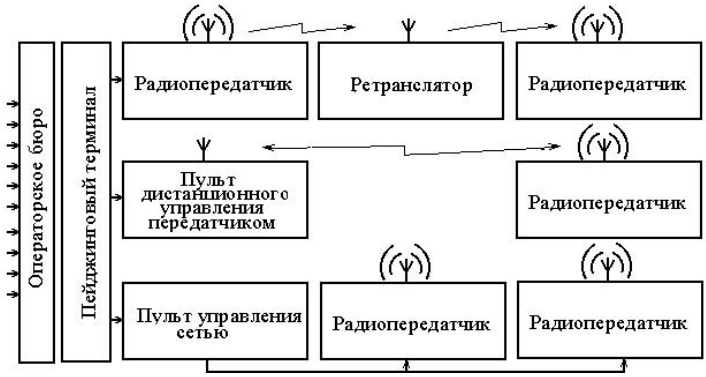


Рисунок 11.1.1 — Структурная схема сети радиопейджинга

обеспечивающие передачу данных по протоколам POCSAG, RDS и FLEX. Примерная структура сети радио-пейджинга представлена на рисунке 11.1.1.

Управление адресацией сообщений выполняется программно, однако если требуется обслужить с одного терминала большое число передатчиков, то на выходе терминала включается пульт управления сетью, который предназначен для управления работой передатчиков радиосети в 4 разных зонах обслуживания.

Пульт дистанционного управления передатчиком предназначен для хранения информации, полученной с терминала до момента получения соединения по коммутируемой линии с передатчиком. Обеспечивает передачу информации от терминала к передатчику по проводной линии или по одночастотному радиоканалу.

Ретранслятор (эхо-репитер) обеспечивает прием информации от основного передатчика и ее передачу по свободному каналу связи, в случае отказа обеспечивает ее хранение в буфере памяти до момента освобождения канала.

Сотовые системы связи

Сотовая связь (СС) отличается от традиционной радиосвязи тем, что в ней не предусматривается создание отдельных, требующих больших затрат энергии каналов связи между каждой парой абонентов. Вместо этого обслуживаемая территория делится на небольшие ячейки (соты) с соответствующим ретранслятором, таким образом, абоненты сети связываются не непосредственно с центральным, а только с ближайшим ретранслятором (рис. 11.1.2).

Принципиальным является то, что ячейки делаются небольшими — радиус действия каждой станции не превышает нескольких километров. В условиях ограниченного диапазона частот тот же самый частотный канал можно использовать снова, но, правда, не в соседней ячейке. Для примера рассмотрим диапазон частот, выделенный для аналоговых систем сотовой связи, емкость которого — 666 телефонных каналов. Оборудование каждой ячейки использует 90 из 666 выделенных частот, т. е. обеспечивает 45 двусторонних телефонных разговоров одновременно.

В соседних ячейках используются другие каналы, а в более удаленных те же самые каналы могут использоваться снова.

Когда абонент сотовой связи «снимает трубку» своего телефона, ближайшая ретрансляционная станция принимает передаваемые телефоном сигналы и выделяет два свободных канала (прием-передача), по которым и осуществляется связь. Вы-

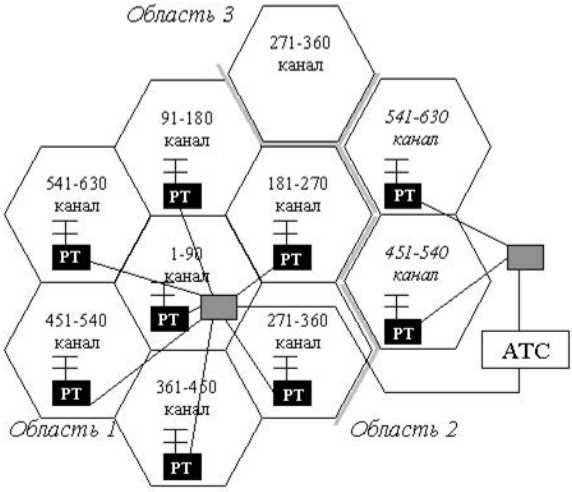


Рисунок 11.1.2 — Структурная схема аналоговой сотовой сети связи

бор каналов полностью автоматизирован — абонент не имеет отношения к этой процедуре. После установки дуплексной связи центральная сотовая станция передает обработку вызова обычной телефонной станции.

В настоящее время сотовые системы связи делятся на два вида: аналоговые и цифровые системы сотовой связи. К середине 1980-х годов аналоговые системы сотовой связи (ACS — *Analog Communication System*) получили достаточно широкое распространение, однако недостаточно высокое качество связи, сложности с шифрованием сообщений и ряд других недостатков, связанных с конфиденциальностью связи, показали, что преодолеть их возможно только на основе цифровой техники.

Переход к цифровым технологиям позволил использовать ряд новых решений, в том числе более эффективные модели повторного использования частот, разнесение во времени процессов передачи и приема при дуплексной связи, шифрование передаваемых сообщений, более эффективные методы интеграции услуг телефонной связи с передачей данных и другими услугами подвижной связи.

Аналоговые системы сотовой связи

Хотя преимущества цифровых СС и определили дальнейшее развитие цифровых систем связи, однако в ряде регионов аналоговые системы продолжают использоваться. К таким системам относятся NMT, AMPS и DAMPS.

NMT-450 — (*Nordic Mobile*). Аналоговый стандарт скандинавской мобильной телефонии NMT-450 использует диапазон частот 453–468 МГц. В этом диапазоне предоставляется значительно большая по сравнению с другими стандартами площадь обслуживания одной базовой станции и соответственно меньшие затраты, а также малое затухание сигнала на открытом пространстве. Недостатком является слабая помехоустойчивость, поскольку в этом частотном диапазоне уровень различного рода помех и их влияние выше, чем в диапазонах 800, 900 и 1800 МГц (особенно ощутимо в больших городах, где развита промышленная сеть). Кроме всего прочего, этот стандарт абсолютно не защищен от прослушивания, поскольку его полоса частот типична для приема ОВЧ-приемника.

AMPS (*Advanced Mobile Phone Service*) — стандарт AMPS рассчитан на диапазон частот 825–890 МГц, характеризуется более высокой, чем у NMT-450, емкостью сетей и более надежной связью в помещениях, низкой восприимчивостью к индустриальным и атмосферным помехам. Однако меньшая зона устойчивой связи для одной базовой станции вынуждает операторов ставить их ближе друг к другу. Учитывая данные недостатки, в стандарте была произведена модернизация на базе цифровых технологий — DAMPS.

Стандарт DAMPS (*Digital Advanced Mobile Phone Service*) с рабочим диапазоном частот 825–890 МГц обладает значительно большей емкостью сетей. В нем сохранена возможность эксплуатации мобильных аппаратов в аналоговом режиме, расширен спектр сервисных услуг, а также емкость сети, хотя и ниже, чем в полностью цифровых системах. Если при роуминге абонент из аналоговой сети AMPS попадает в цифровую — DAMPS, для работы ему выделяются аналоговые каналы, однако в этом случае преимущества цифровой связи недоступны.

Цифровые системы сотовой связи

Существует несколько стандартов цифровых систем связи: европейский GSM (*Global System for Mobile communications*), американский традиционно использующийся в США PCS (Personal Communications Service), английский DCS-1800 (DCS — *Digital Cellular System*), являющийся прямым аналогом GSM-1800, японский JDS (*Japan Digital System*) и CDMA (*Code Division Multiple Access*).

GSM (*Global System for Mobile communications*). Это стандарт, определяющий работу в радиотелефонных сетях общего пользования. В России для работы сотовых систем общего пользования систем GSM выделен частотный диапазон 900 МГц. Стандарт GSM-900 (как, впрочем, и NMT-450i) получил статус федерального. Сеть GSM 900 работает в диапазонах частот 900 (или 1800) МГц. В диапазоне 900 МГц подвижной абонентский аппарат передает на одной из частот в диапазоне 890–915 МГц, а принимает на частотах 935–960 МГц. В дуплексном канале, состоящем из восходящего и нисходящего направлений передачи, для каждого из названных направлений применяются частоты, различающиеся точно на 45 МГц. В каждом из указанных выше частотных диапазонов создаются по 124 радиоканала (124 для приема и 124 для передачи данных, разнесенных на 45 МГц) шириной по 200 кГц каждый. Этим каналам присваиваются номера (N) от 0 до 123.

В распоряжение каждой базовой станции может быть предоставлено от одной до 16 частот, причем число частот и мощность передачи определяются в зависимости от местных условий и нагрузки.

В каждом из частотных каналов, которому присвоен номер (N) и который занимает полосу 200 кГц, организуются восемь каналов с временным разделением (временные каналы с номерами от 0 до 7) или восемь канальных интервалов.

Система с уплотнением каналов по частоте позволяет получить 8 каналов по 25 кГц, которые, в свою очередь, уплотняются по времени излучения еще на 8 каналов. В стандарте GSM несущая частота сигнала изменяется 217 раз в секунду для того, чтобы компенсировать возможное ухудшение качества. Поэтому, когда абонент получает канал, ему выделяется не только частотный канал, но и один из строго отведенных временных интервалов, — иначе создаются помехи в других каналах. В соответствии с вышеизложенным, работа передатчика происходит в виде отдельных импульсов, которые происходят в строго отведенном канальном интервале: продолжительность канального интервала составляет 577 мкс, а всего цикла — 4616 мкс. Выделение абоненту только одного из восьми канальных интервалов позволяет разделить во времени процесс передачи и приема путем сдвига каналь-

ных интервалов, выделяемых передатчикам подвижного аппарата и базовой станции. Базовая станция всегда передает на три канальных интервала раньше подвижного аппарата.

Таким образом, последовательность импульсов, которая образует физический канал передачи GSM, характеризуется номером частоты и номером временного канального интервала. На основе этой последовательности импульсов организуется целая серия логических каналов, которые различаются своими функциями. Кроме каналов, передающих полезную информацию, стандартом предусматривается ряд каналов, передающих сигналы управления, а также организация прямой двусторонней связи с сотовыми терминалами (или цифровыми устройствами обработки информации). Подобные технологии различаются по наличию инфракрасного (IR-ID) или радиочастотного (Bluetooth,, ZigBee и т. п.) интерфейсов малого радиуса действия, которые предназначены для связи находящихся рядом устройств. Большая часть сценариев подобных интерфейсов включает вариант, когда одно из устройств является устройством беспроводной коммуникации стандарта WAP. Реализация таких каналов и их работа находятся под управлением операционной системы (ОС) абонентских устройств.

В виду того, что многие устройства Bluetooth могут являться участниками телеконференций (WAP Forum), существует реальная угроза вирусной атаки ОС сотовых терминалов. По данным компании F-Secure, проникновение вируса Cabir на мобильные телефоны уже было зарегистрировано на Филиппинах, в Сингапуре, Арабских Эмиратах, Китае, Индии, Финляндии, Турции и Вьетнаме. В качестве первого российского носителя сетевого червя выступил телефон Nokia 7610. Анализ содержащейся в мобильном телефоне информации показал, что вредоносный код полностью идентичен оригинальному варианту Cabir, обнаруженному в июне 2004 года. Это дает основания для неутешительного вывода — сетевой червь уверенно распространяется по всему миру, инфицируя мобильные телефоны Symbian OS.

CDMA (*Code Division Multiple Access*) — система цифровой сотовой связи с кодовым разделением каналов на основе использования шумоподобных сигналов. В отличие от других цифровых систем, которые делят отведенный диапазон на узкие каналы по частотному (FDMA) или временному (TDMA) признаку, в стандарте CDMA передаваемую информацию кодируют и код превращают в шумоподобный широкополосный сигнал так, что его можно выделить снова, только располагая кодом на приемной стороне. При этом одновременно в широкой полосе частот можно передавать и принимать множество сигналов, которые не мешают друг другу. Основой метода разделения каналов с реализацией многостанционного доступа с кодовым разделением CDMA-1 (в реализации компании *Qualcomm*) является расширение спектра методом прямого кодирования последовательности данных последовательностями Уолша (*Walsh Coding*).

Одно из преимуществ цифровой связи с шумоподобными сигналами — защищенность канала связи от перехвата, помех и подслушивания. Именно поэтому данная технология была изначально разработана и использована для вооруженных сил США, и лишь совсем недавно американская компания Qualcomm на основе этой технологии создала стандарт IS-95 (CDMA-1) и передала его для коммерческого использования.

Как уже указывалось, технология CDMA обеспечивает высокое качество сигнала при снижении излучаемой мощности и уровня шумов. В результате можно добиться минимальной средней выходной мощности, значение которой в сотни раз меньше значений выходной мощности других, используемых в настоящее вре-

мя стандартов. Это позволяет уменьшить воздействие на организм человека и увеличить продолжительность бесперебойной работы без подзарядки аккумулятора. Так, излучаемая мобильными аппаратами средняя мощность в сотовых системах CDMA составляет менее 10 мВт, что на порядок ниже мощности, требуемой, например, в системах с временным разделением каналов TDMA. Эффективное использование радиочастотного диапазона с возможностью многократного использования одних и тех же частот в сети (высокая спектральная эффективность) увеличивает емкость CDMA в 10–20 раз по сравнению с аналоговыми системами и в 3–6 раз превышает плотность других цифровых систем.

Наконец, в стандарте предусмотрен плавный переход между сотами (или секторами в пределах одной соты), что позволяет осуществлять «мягкий» переход от одной соты к другой, в отличие от GSM, где такой переход происходит скачкообразно, что приводит к короткому временному разрыву соединения.

Развитие цифровых систем связи предполагает создание нового четвертого поколения (4G) сотовых систем связи. На сегодня 3G-технологии представлены в выборе из 3 стандартов:

– W-CDMA (*Wide Band Code Division Multiple Access*), предусматривающий переход к 3G от технологий GSM;

– cdma2000 (компании *Qualcomm*), которая ориентирована на замену технологии CDMA-1 (*cdmaOne*);

– DoCoMo — японская система, согласованная с W-CDMA, ориентированная на переход с систем, использующих временной (TDMA) принцип разделения каналов (*Time Division Multiple Access*).

Несмотря на неопределенность в выборе конкретного стандарта, Институт Европейских Стандартов Телекоммуникаций уже разрабатывает соответствующий стандарт UMTS (*Universal Mobile Telecommunications System*). Так, для UMTS-систем выделены два частотных диапазона — 1885–2025 МГц и 2110–2200 МГц. Определен набор функциональных возможностей средств связи, к наиболее важным функциям отнесены:

– речевые вызовы;
– видеотелефония;
– IP-телефония;
– передача видеоизображения в режиме «live» по WAP протоколу;
– трансляция аудио-репортажа;
– прием телевизионных программ;
– видео- и фотосъемка;
– скоростной доступ к сети Internet, включая WEB-браузинг с использованием технологий WAP и GRPS;
– мобильный офис;
– определение местоположения абонента по картам и путеводителям;
– электронная почта, шопинг и коммерция.

Очевидно, для обеспечения, перечисленного в абонентском терминале 3G должна быть видеокамера. Для просмотра телепрограмм необходим цветной жидкокристаллический экран достаточно большого размера. Услуги мобильного офиса, а также игры требуют высокопроизводительного процессора, большой памяти и удобных клавиатуры и манипулятора. Работа всех этих устройств должна обеспечиваться батареей электропитания достаточно большой емкости. И, главное, такой прибор должен быть очень компактным, не превосходящим по размеру привычный сотовый телефон.

Предполагается, что по исполнению радиосредства, разрабатываемые для 3G, будут делиться на две категории: интеллектуальные телефоны и электронные органайзеры. Сегодня примером первых могут служить аппараты, сочетающие в себе мобильный телефон и карманный компьютер. Вторые лучше всего можно представить органайзерами типа Palm, оснащенными средствами беспроводной передачи данных (рис. 11.1.3).

а) б)

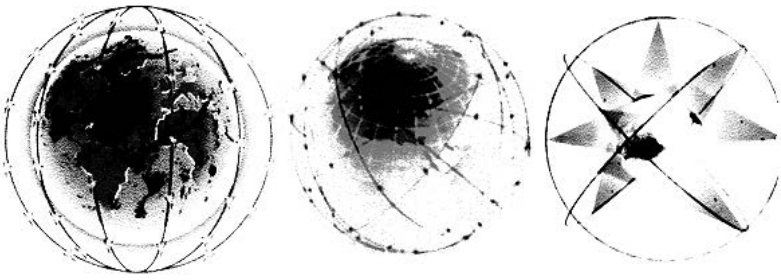
Рисунок 11.1.3 — Телекоммуникационные устройства нового поколения:
а) универсальные терминалы связи от Siemens;
б) цифровые фотоприставки к сотовым телефонам от Codak

Первая фаза 3G подходит к завершению и в некоторых европейских странах уже выданы лицензии на эксплуатацию UMTS, многие производители уже выпускают портативные телефоны со встроенными видеокамерами, TV-дисплеями и скоростью передачи данных, превышающей 64 кбит/с.

Спутниковые средства связи

Строение и принцип работы сети спутниковой связи напоминает собой структуру сотовой связи, в которой зональные (сотовые) ретрансляторы находятся на орбитальных спутниках земли. Спутниковые системы связи, ориентированные на обслуживание сетей связи общего пользования, базируются на искусственных спутниках земли (ИСЗ), находящихся на так называемых низких орбитах ≈1000 км. Такая высота расположения спутника по сравнению со стационарной орбитой размещения дает возможность почти в 1600 раз снизить мощность радиосигнала, что позволяет понизить требования к приемным и антенным системам абонентских терминалов.

В этом заключается главное преимущество низкоорбитальных систем связи (НСС). Однако, в отличие от стационарных орбит, на которых ИСЗ вращается вместе с Землей, низкоорбитальные спутники движутся по орбите со скоростью около 7 км/с. При таких условиях время видимости спутника не превышает 14 минут, после чего спутник «уходит» за линию горизонта. Поэтому для поддержки непрерывной связи (например, при телефонном разговоре) необходимо, чтобы в тот момент, когда первый спутник покидает зону обслуживания, на смену ему приходил второй, за ним — третий и т.д. Таким образом, для надежного охвата всей территории Земли необходимо большое количество спутников, примерно несколько десятков, хотя известны проекты, в которых их число приближается к тысяче. Рас-



а) б) в)

Рисунок 11.1.4 — Спутниковые низкоорбитальные группировки:
а) орбитальная группировка Иридиум; б) орбитальная группировка Глобалстар;
в) орбитальная группировка Одиссей

положение орбит наиболее разработанных систем спутниковой связи представлено на рисунке 11.1.4.

Для того, чтобы обеспечить связью абонентов не только внутри зоны видимости, но и на всей территории Земли, соседние спутники могут связываться между собой и передавать информацию по цепочке, пока она не дойдет до адресата. С этой целью, как правило, используются наземные шлюзовые станции, которые также выполняют функцию средств сопряжения с обычными наземными сетями связи.

Проекты низкоорбитальных глобальных систем связи в значительной степени отличаются друг от друга как орбитальными характеристиками, так и различными предусмотренными сервисами связи. К наиболее разработанным из них относятся проекты Иридиум, Глобалстар и Inmarsat-P, которые имеют сходство по принципу работы, но отличаются более высокими орбитами.

Проект Иридиум реализуется международным консорциумом Iridium Inc., созданным фирмой Motorola с участием таких фирм, как Lockheed, Douglas и другими. Активное участие в проекте принимает Государственный космический научно-производственный центр им. М.В. Хруничева. Он является одним из учредителей консорциума.

Проект Глобалстар реализуется международным консорциумом LQSS (*Loral Qualcomm Satellite Services*) при участии ряда других фирм.

Все перечисленные системы глобальной низкоорбитальной спутниковой связи предлагают примерно одинаковый набор услуг, к ним относятся:

- передача речи (телефония);
- передача факсимильных сообщений;
- передача данных;
- служба голосовой почты;
- персональный радиовызов (пейджинг);
- определение местоположения абонента.

Структура спутниковых каналов передачи данных может быть проиллюстрирована на примере широкоизвестной системы VSAT (*Very Small Aperture Terminal*) (рис. 11.1.5).

Наземная часть системы (центральная станция ЦС) представлена совокупностью приемопередающего оборудования, включающего направленную антенну диаметром 1 ... 3 м и коммутационной аппаратуры связи с абонентскими терминалами

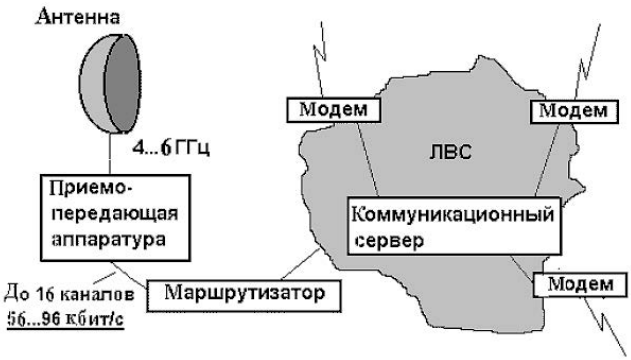


Рисунок 11.1.5 — Пример структурной схемы системы спутниковой связи

(АТ) связи. АТ подключаются к ЦС по схеме «звезда» с помощью многоканальной аппаратуры по проводным или радиоканалам связи.

Каналы спутниковой подвижной связи работают в диапазонах частот 137–900 МГц и 1970–2520 МГц, что практически не отличается от частот сотовой связи (450–1800 МГц).

Средняя мощность абонентского носимого радиотелефона невелика и составляет, например, для терминала Иридиум порядка 13–40 мВт, для стационарного — до 400 мВт — это означает, что спутниковый телефон не более опасен, чем привычный сотовый. В терминалах спутниковой связи предусмотрено сопряжение с сетями сотовой связи, что обеспечивается вставляемой в терминал идентификационного устройства SIM-карты.

§ 2. Состав и особенности работы средств радиотелефонной связи ОВД

Система радиотелефонной связи ОВД с мобильными объектами основана на базе радиостанций ОВЧ-диапазона и является симплексной многоканальной системой, обеспечивающей связь на любом из 80 каналов, расположенных в одном из двух поддиапазонов (диапазон А — 148–149 МГц; диапазон Б — 172–173 МГц).

Основными средствами связи являются различные радиостанции («Сапфир», «Транспорт», «Motorola») в стационарном, возимом и носимом вариантах исполнения. Рассмотрим для примера комплект радиостанций системы «Сапфир». В систему входят:

- диспетчерская радиостанция — ДСР;
- стационарные радиостанции — АСР-1,2;
- возимые радиостанции — АВР-1,2;
- переносная радиостанция — «Вояж»;
- программатор каналов — «Стрелец-1».

Диспетчерская радиостанция ДСР комплекса «САПФИР»

Предназначена для организации многоканальной радиосвязи дежурных частей. Обеспечивает одно- и двухчастотный симплексный режим, подключение к АТС, регистрирующим устройствам, резервному питанию, программирование информации, отображение индивидуального кода радиостанции на пульте, текущего времени и другие функции. Имеет дистанционое управление, охранную сигнализацию пери-

ферийного оборудования, дублирующий пульт. Комплектуется широкополосной антенной (АСНЕ) и универсальным приемопередатчиком комплекса «Сапфир».

Стационарная радиостанция АСР-1 комплекса «САПФИР»

Предназначена для организации радиосвязи стационарных объектов служб и подразделений МВД. Обеспечивает работу в одно- и двухчастотном симплексном режиме, имеет возможность посылки до пяти индивидуальных вызовов, автоматическое ограничение времени непрерывной работы передатчика и др. Комплектуется широкополосной антенной (АСНЕ).

Все радиостанции комплекса характеризуются следующими характеристиками:

- полная (пониженная) мощность передатчика, Вт — 10(2);
- чувствительность приемника, мкВ — 0,2–0,5;
- число программируемых каналов — 160.

Стационарная радиостанция АСР-2 комплекса «САПФИР»

Предназначена для организации адресной радиосвязи стационарных объектов служб и подразделений МВД. Обеспечивает работу в режиме одно- и двухчастотного симплекса и «дежурный прием», посылку индивидуального кода в режиме «передача» и до 100 000 индивидуальных вызовов, автоматическое ограничение времени работы передатчика. Комплектуется широкополосной антенной (АСНЕ). Имеет вариант разнесенного пульта управления.

Возимая радиостанция АВР-1 комплекса «САПФИР»

Предназначена для обеспечения радиосвязью сотрудников ОВД на автомобилях. Обеспечивает работу в одно- и двухчастотном симплексном режиме, посылку индивидуального кода в режиме «передача» и до 5 индивидуальных вызовов, автоматическое ограничение времени непрерывной работы передатчика, защиту от короткого замыкания и переполюсовки по питанию. Информация о каналах и частотах программируется. Возможны варианты поставки с разнесенным пультом управления и блоком преобразования напряжения.

Возимая радиостанция АВР-2 комплекса «САПФИР»

Предназначена для организации радиосвязи подвижных объектов и подразделений МВД. Обеспечивает работу в одно- и двухчастотном симплексном режиме, «дежурный прием», поиск сигнала по 4 каналам, посылку индивидуального кода в режиме «передача» и до 100 000 индивидуальных вызовов, автоматическое ограничение времени работы передатчика и др. Возможны варианты поставки с разнесенным пультом управления и блоком пребразования напряжения.

Переносная радиостанция «ВОЯЖ» комплекса «САПФИР»

Предназначена для организации радиосвязи на месте происшествия. Обеспечивает работу в режиме одно- и двухчастотного симплекса, режим ретрансляции при соединении 2 радиостанций, питание от сети и от встроенных аккумуляторов, др. возможности. Комплектуется комбинированной выносной магнитной антенной.

Программатор «СТРЕЛЕЦ-1»

Предназначен для занесения данных о распределении частот по каналам, режимах работы и индивидуальных номерах радиостанций комплекса «Сапфир».

Программатор состоит из ПЭВМ (черно-белого монитора с блоком питания, клавиатуры и блока интерфейса). Разработана программа для IBM-совместимого компьютера, позволяющего выбрать радиосредства комплекса «Сапфир», соответствующие требованиям и условиям эксплуатации.

Носимая радиостанция «РАДИЙ»

Предназначена для организации связи пеших абонентов между собой, а также с подвижными и стационарными корреспондентами.

Обеспечивает работу в режиме одно- и двухчастотного симплекса, посылку групповых вызовов, предварительное программирование радиостанций пользователем и другие возможности.

Диапазон рабочих частот, МГц	140–174; 204–212
Количество каналов	не более 80
Минимальный разнос частот между каналами, кГц	25
Максимальный разнос частот между каналами, МГц	2,5
Габаритные размеры (аккумуляторной батареи), мм	166 × 68 × 37

§ 3. Порядок настройки и работы с радиотелефонными средствами

Порядок работы с автомобильной радиостанцией «Motorola GM-300» (рис. 11.3.1)

1. Включение/выключение радиостанции.

Включить радиостанцию, повернув ручку регулировки громкости до щелчка по часовой стрелке. Производится самоконтроль, на мониторе указывается последнее состояние радиостанции и раздается звуковой сигнал. Если раздается сигнал неисправности, обратитесь к специалисту связи.

Выключить радиостанцию, повернув ручку регулировки громкости против часовой стрелки.

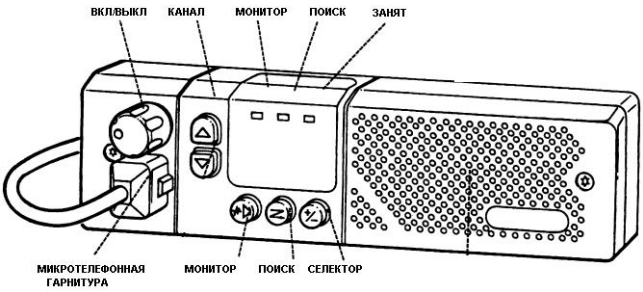


Рисунок 11.3.1 — Панель управления радиостанцией «Motorola GM-300»

2. Прием радиосигналов:

Установить уровень громкости, повернув ручку регулировки громкости по часовой стрелке.

Выбрать канал при помощи кнопок «вверх/вниз». Продолжительное нажатие повлечет прокрутку каналов.

Для контроля канала нажать кнопку «монитор» или снять микрофон с фиксатора. В режиме контроля должен постоянно гореть желтый светодиод — монитор.

Для отключения режима автоматической настройки нажать и держать кнопку «монитор» в течение 2 с.

Для выхода из режима без автонастройки — нажать кнопку «монитор» снова. Это возвратит радиостанцию в режим кодированной настройки частотной линии.

3. Передача:

Перед передачей нажать кнопку контроля для того, чтобы проверить, что канал свободен. Если канал свободен, нажать тангенту микрофона и говорить медленно

и четко. Светодиод передача/занят останется красным, пока тангента микрофона не будет отпущена.

Красный светодиод передача/занят будет мигать, если на выбранном канале есть другая несущая.

Порядок работы с носимой радиостанцией «Motorola GP-300» (рис. 11.3.2)

1. Включение/отключение радиостанции.

Повернуть ручку регулировки громкости по часовой стрелке до звукового сигнала, говорящего о том, что радиостанция готова к работе.

Для выключения радиостанции повернуть ручку громкости против часовой стрелки до упора после щелчка.

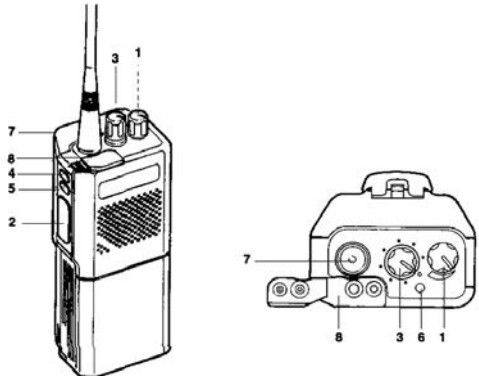


Рисунок 11.3.2 — Панель управления носимой радиостанцией «Motorola GM-300»: 1. Ручка регулировки громкости. 2. Включение/выключение радиостанции. 3. Тангента. 4. Ручка переключателя каналов. 5. Кнопка (без запрограммированной функции). 6. Кнопка (без запрограммированной функции). 7. Индикатор. 8. Антенна. 9. Соединительное гнездо для выносных манипуляторов

2. Передача сигналов:

Установить переключателем каналов требуемый канал.

Прослушать канал связи (он должен быть свободен).

Удерживать радиостанцию в вертикальном положении с решеткой громкоговорителя-микрофона на расстоянии 5–8 см ото рта.

Нажать кнопку передачи сбоку, говорить в микрофон (по окончании передачи отпустить кнопку для приема ответных сообщений).

3. Прием:

Установить переключателем каналов требуемый канал.

Прослушать передачу и отрегулировать громкость на подходящий уровень.

4. Смена аккумулятора:

Перед тем, как вынимать аккумулятор, выключить радиостанцию. Нажать затвор аккумулятора в сторону передней панели радиостанции, продвинуть аккумулятор вниз приблизительно на 2 см и вынуть его из радиостанции.

Для того, чтобы установить аккумулятор, необходимо вставить его в направляющие и продвинуть к верхней поверхности, пока не закроется затвор аккумулятора.

Тема 12. ОПЕРАТИВНО-СЛУЖЕБНЫЙ ТРАНСПОРТ

§ 1. Роль специального транспорта в решении задач по обеспечению общественного порядка и борьбы с преступностью

Выполнение оперативно-служебных задач службами и подразделениями ОВД связано с необходимостью использования специальных транспортных средств для быстрого перемещения сил и средств, а также перевозки арестованных. Известно, что в раскрытии преступлений важную роль играет фактор времени. Чем быстрее прибудет оперативная группа на место происшествия и чем больше в ее арсенале окажется приборов специальной техники, тем эффективнее ее оперативно-служебная деятельность, т. е. быстрее и всестороннее раскрытие преступления. Трудно представлять сейчас работу дежурных частей ОВД без специальных автомобилей и мотоциклов. Без специального транспорта почти невозможно организовать четкую работу патрульной службы, ГИБДД, конвойной охраны и медицинских вытрезвителей.

Наличие большого количества специального транспорта в ОВД привело к необходимости реорганизации патрульно-постовой службы, к созданию подвижных патрульных полицейских групп.

Правильное использование специального транспорта обеспечивает:

– бóльшую подвижность и мобильность патрульно-постовых служб;

– возможность оперативно маневрировать имеющимися силами в соответствии со сложившейся оперативной обстановкой;

– эффективную охрану общественного порядка на значительной территории с меньшим количеством личного состава;

– быструю и своевременную переброску сил и средств при выполнении специальных операций;

– своевременное проведение оперативно-розыскных мероприятий и следственных действий (СОГ);

– размещение пунктов управления служебными нарядами при проведении массовых мероприятий;

– проведение агитационной и профилактической работы.

Эффективность применения специальных автомобилей, мотоциклов, катеров, вертолетов в значительной степени повышается при оснащении их дополнительным специальным оборудованием (средствами связи, громкоговорящими установками, световыми проблесковыми маяками, звуковыми и световыми специальными сигналами, радиолокационными измерителями скорости и другими приборами специальной техники).

§ 2. Виды специального транспорта и их назначение при осуществлении различных оперативно-служебных мероприятий

В соответствии с задачами и назначением оперативно-служебный транспорт можно подразделить на следующие группы:

– специальные транспортные средства дежурных частей;

– специальные транспортные средства для патрулирования (ППС, ДПС);

– специальные транспортные средства для перевозки арестованных (автозак);
– специальные транспортные средства для обеспечения массовых мероприятий;
– специальные транспортные средства для оперативных подразделений;
– специальные транспортные средства для проведения специальных операций;
– специальные транспортные средства для проведения криминалистических исследований (передвижные криминалистические лаборатории)

В качестве специального автомототранспорта применяются серийные автомобили и мотоциклы, оборудованные специальными кузовами, дополнительными устройствами, приспособлениями и техническими средствами.

Для обеспечения работы передвижных патрульных групп полиции в основном используются автомобили типа УАЗ-469 со специальным цельнометаллическим кузовом, ГАЗ-24 «Волга» и ее модификации, различные модели автомашин марок «Жигули», «Москвич», а также тяжелые мотоциклы марок «Урал», «Ирбит». Все эти автомототранспортные средства имеют специальную окраску в соответствии с ГОСТом, а также дополнительное оборудование: ОВЧ-радиостанции, сигнально-громкоговорящие установки.

В районах с суровыми климатическими условиями могут использоваться и иные виды патрульного автомототранспорта: мотосани типа «Буран», вездеходы колесного и гусеничного типа и даже гужевой транспорт (в условиях бездорожья).

Для автомототранспортного обеспечения оперативно-розыскных аппаратов используются обычные серийные автомашины марок «Волга», «Жигули», «Москвич», УАЗ-469 и другие, не имеющие специальной окраски и ознакомительных знаков полиции. Для обеспечения конспирации оперативно-розыскной деятельности средства ОВЧ-радиосвязи и спецсигналы устанавливаются скрытно. Так, штатная антенна радиостанции заменяется эквивалентом с выходом на обычную антенну автомобильного приемника или скрытно размещается в деталях кузова. Маскируется пульт управления и другие блоки радиостанции.

В настоящее время для оперативно-розыскных аппаратов поставляют автомашины марок «Волга» и «Жигули» специального исполнения, оборудованные форсированным двигателем повышенной мощности, имеющие усиленный кузов и улучшенную трансмиссию. Такие автотранспортные средства предназначены для обеспечения ведения скрытного наблюдения.

Специальным автотранспортом оснащаются и дежурные части ОВД. Такие автомашины создаются на шасси УАЗ-452 или микроавтобуса РАФ, оборудуются специальным кузовом, имеющим отсеки для работы оперативно-следственной группы, перевозки задержанных, служебно-розыскных собак. Кроме того, здесь имеются специальные приспособления для фотосъемки с крыши автомобиля, освещения места происшествия и т. д. В комплектацию автомашины дежурной части (АДЧ) входят различные средства связи, специальной и криминалистической техники, вспомогательные устройства и приспособления, необходимые для обеспечения работы следственно-оперативной группы на месте происшествия в различных условиях.

Специальный автотранспорт имеется и в подразделениях ГИБДД. Как правило, это типовые автомашины марок «Волга», «Жигули» и микроавтобусы РАФ. В сельской местности широко используются автомашины повышенной проходимости типа УАЗ-469 и УАЗ-452. Все они имеют специальную окраску с отличительной надписью «ГИБДД». Эти автомашины оснащаются средствами связи, сигнально-громкоговорящей установкой, а также могут быть укомплектованы радиолокационными измерителями скорости, диагностической аппаратурой контроля исправности

автомототранспорта, приборами для обнаружения алкогольного опьянения у водителей и другой специальной техникой ГИБДД.

Кроме того, органами ГИБДД применяются: специальные агитационные автобусы для пропаганды правил уличного движения, оснащенные средствами наглядной агитации, звукоусиления, кинопроекционной аппаратурой и т. п.; автобусы для проведения в сельской местности регистрационной работы и приема экзаменов на право управления автомототранспортом; передвижные диагностические лаборатории; автомашины для выезда на место автодорожного происшествия.

В последние годы широкое применение на крупных автомагистралях нашли такие транспортные средства как вертолеты. Их техническая эксплуатация и управление осуществляются силами подразделений гражданской авиации, но под руководством специально выделенных сотрудников ГИБДД.

Для обеспечения перевозки арестованных и подследственных также используются специальные автотранспортные средства различного типа на шасси грузовых автомашин ГАЗ-53 или ГАЗ-66. Они имеют специальный цельнометаллический кузов, разделенный внутри на индивидуальные отсеки для конвоируемых и отсек для конвоя.

Такие автомашины дополнительно оборудуются переговорными устройствами для связи между отсеком конвоя и кабиной водителя, ОВЧ-радиостанцией, проблесковым маяком.

Для массовой перевозки осужденных (например, на производственные объекты и обратно) используются специальные автомашины с двумя отсеками; в одном размещаются осужденные, в другом — конвой. В отдельных случаях (например, при захвате вооруженных преступников) используются бронетранспортеры. Для обслуживания водных акваторий соответствующие подразделения полиции оснащаются быстроходными катерами на подводных крыльях или на воздушной подушке, маломерными речными и морскими судами.

Тема 13. ТЕХНИЧЕСКИЕ СРЕДСТВА ДЕЖУРНЫХ ЧАСТЕЙ

§ 1. Назначение и виды технических средств дежурных частей

В деятельности дежурных частей как ни в каком другом практическом органе просматривается необходимость комплексного использования технических средств управления и специальной техники.

Дежурные части предназначены обеспечивать сбор данных об оперативной обстановке на обслуживаемой территории и незамедлительно реагировать на заявления и сообщения о правонарушениях, проводить объективное разбирательство по горячим следам при условии строгого соблюдении законности.

Структурное построение и штатная численность дежурных частей регламентируются ведомственными нормативными актами и зависят от уровня, занимаемого конкретными подразделением в единой системе управления, а также от количества подчиненных органов. Нормативными актами определены также задачи и функции дежурных частей.

По характеру и объему задач дежурные части классифицируются на 2 категории. К первой категории относятся дежурные части центральных аппаратов федеральных министерств и ведомств, субъектов Российской Федерации, главных управлений по округам, по городам с населением более 1 миллиона человек. Ко второй категории — дежурные части отделов, отделений по территориальным муниципальным образованиям, т. е. районного масштаба.

Основными принципами работы дежурных частей являются: высокая боеготовность, оперативность, гибкость управления подчиненными силами и средствами; глубокое знание оперативной обстановки на обслуживаемой территории; преемственность в работе; соблюдение законности; сохранение служебной тайны; четкое выполнение нормативных актов; профессиональная бдительность; вежливость и уважительное отношение к гражданам.

Качественное выполнение стоящих перед дежурными частями ОВД задач по управлению подчиненными силами и средствами в охране общественного порядка и борьбе с преступностью достигается: высоким профессионализмом сотрудников; тщательно разработанными планами их действий при изменениях оперативной обстановки; достаточным техническим и материальным обеспечением.

В деле совершенствования деятельности дежурных частей особо следует подчеркнуть повышение роли научных методов и технических средств (систем) управления, специальной техники.

Коренное изменение отношения к техническому обеспечению деятельности дежурных частей обусловлено:

– значительным усложнением объектов управления;

– требованиями существенного расширения круга и повышения достоверности сведений о характеристиках управляемого объекта;

– необходимостью обеспечения принятия оперативных решений своевременно и с достаточной обоснованностью.

С позиций целевого подхода техническое обеспечение деятельности дежурных частей можно разбить на ряд групп технических средств:

– системы связи;
– специальные средства и вооружение;
– системы охраны и телевизионного наблюдения;
– управляющие автоматизированные комплексы.

Представленные основные группы технических средств, применяемых в дежурных частях, охватывают все многообразие различной по назначению техники. Каждое из технических средств предназначено для выполнения одной или нескольких частных задач и функций, стоящих перед дежурными частями. В целом работа дежурных частей обеспечивается комплексным использованием всех технических средств, состоящих на вооружении.

Именно комплексность технических средств, полное их соответствие поставленным тактико-техническим требованиям, разумное резервирование и постоянное технологическое обновление их являются основным направлением совершенствования деятельности дежурных частей. В свою очередь, такой подход служит делу дальнейшего повышения эффективности управления ОВД.

Для обеспечения централизованного управления техническим комплексом дежурных частей создается оперативный пункт управления и в нем оборудуются рабочие места для оперативных дежурных и их помощников. Техническая база управления наряду с электронно-вычислительной техникой включает в себя средства оперативной связи, аппаратуру оповещения личного состава, средства звуко- и видеозаписи, устройства охранной и пожарной сигнализации, телевизионную и другую технику.

Данный комплекс технических средств позволяет дежурным частям оперативно и в полном объеме решать задачи. В значительной степени эффективность работы системы управления деятельностью ОВД зависит от качества и надежности применяемых средств и систем связи.

Для решения задач управления организуются узлы (пункты) связи, которые структурно входят в состав дежурных частей. Такие узлы связи можно осуществлять автоматический прием сообщений о происшествиях, осуществлять взаимодействие и поддерживать непрерывную связь с подвижными объектами (абонентами).

В состав узла связи входят:

– пульты, станции, коммутаторы оперативной связи, в которые включаются внутренние и внешние телефонные линии;
– учрежденческая автоматическая телефонная станция;
– линии привязки к узлам связи Министерства связи и массовых коммуникаций Российской Федерации и других министерств и ведомств;
– радиостанции;
– телефонные аппараты городской и ведомственной связи;
– аппаратура магнитной записи;
– средства телевидения;
– специальные изделия, аппаратура, устройства.

Наиболее распространенными видами связи, используемыми в работе дежурных частей, являются средства проводной связи и радиосвязи.

Рассматривая организацию и особенности осуществления телефонной проводной связи, необходимо отметить, что в настоящее время дежурные части обеспечиваются этим видом связи на правах приоритетных служб. Основой организации проводных линий связи в МВД РФ является использование каналов общегосударственной сети, ведомственных и собственных линий связи.

Дежурному персоналу практически повсеместно предоставлена возможность установления телефонной связи как с подчиненными данному органу управления подразделениями, так и со взаимодействующими ОВД. При этом используются возможности специальной и обычной междугородной автоматической, заказной или по паролю связи, местной городской и учрежденческой автоматической связи, прямой автоматической — для обмена оперативной информацией и местной, входящей по спецлиниям «02» — для приема сообщений о происшествиях, для непосредственного управления силами и средствами.

Используется также ряд дополнительных устройств, способствующих выполнению персоналом своих функций: 1) устройство автонабора; 2) определение номера абонента; 3) удержание абонента на связи с автоответчиком и др.

В системе МВД РФ документальная передача информации производится с использованием средств телеграфной связи. В зависимости от оснащенности ОВД аппаратурой, наличия предоставленных в аренду местными предприятиями Министерства связи и массовых коммуникаций Российской Федерации каналов связи, информация передается одним из следующих способов:

– по телеграфной сети общего пользования, организуемой между предприятиями Министерства связи и массовых коммуникаций Российской Федерации;

– по сети абонентского телеграфирования, организуемой между предприятиями и учреждениями;

– по ведомственной сети телеграфной связи, организуемой по арендуемым каналам связи.

Положительно зарекомендовало себя уплотнение арендуемых телефонных каналов, при котором абонентам предоставлены один телефонный и два телеграфных канала связи.

В ряде УВД используется аппаратура циркулярной передачи телеграфных сообщений. В настоящее время в ОВД эксплуатируются различные типы телеграфных аппаратов электромеханического и электронного принципа действия. Наиболее перспективными являются ***телеграфные аппараты РТА-80*** и ***Т-100,*** которые поступают на вооружение органов.

Большие возможности перед службами ОВД и, прежде всего, перед дежурными частями в вопросах повышения оперативности и достоверности получения данных, используемых для предотвращения и раскрытия преступлений, розыска преступников, открывает использование факсимильной связи для передачи и приема информации в документальном виде. Современные факсимильные телетайпы (аппаратура приема и передачи информации) позволяют передавать без искажений графическую, текстовую, знаковую и рисованную от руки информацию с четкостью, достаточной для идентификации человека или дактилоскопического отпечатка. В Российской Федерации с целью создания факсимильной техники на современном мировом уровне проводится разработка аппаратуры, в которой предусмотрены новейшие достижения в этой области ведущих зарубежных фирм («Канон», «Панасоник», «Рико» — Япония).

Наиболее распространенным и оперативным видом передачи речевой информации подвижным и рассредоточенным объектом в системе МВД РФ является радиосвязь в ОВЧ и ВЧ-диапазонах. Средства ОВЧ-радиосвязи представлены стационарными, мобильными и носимыми радиостанциями. Связь радиосредствами в дежурных частях организуется по радиосетям и радионаправлениям. В радиосетях и радионаправлениях радиостанция дежурной части является главной радиостанцией; ее требования выполняются всеми радиостанциями радиосети.

Для обеспечения и установления радиосвязи дежурным частям назначаются следующие данные: частоты: позывные, тональный вызов, время связи, кодовые таблицы. Варианты радиоданных разрабатываются заблаговременно и доводятся до подчиненных органов и подразделений внутренних дел.

Важным оперативно-техническим элементом в деятельности дежурных частей является ведение магнитофонной записи поступающей речевой информации и отдаваемых распоряжений.

В этих целях в дежурных частях МВД, УВД применяются многоканальные магнитофоны, с помощью которых обеспечивается круглосуточная запись информации, циркулирующей по подключенным к ним телефонным и радиоканалам связи. Из применяемых многоканальных магнитофонов в дежурных частях наибольшее распространение получили ***«ШХР»*** (Венгрия) и ***«Спектр»*** (Россия). Решается вопрос об оснащении дежурных частей горрайорганов внутренних дел — наиболее многочисленной группы пользователей — 4-канальными магнитофонами.

Применение аппаратуры магнитной записи для фиксации информации позволило существенно повысить четкость реагирования персонала дежурных частей на поступающие сообщения о происшествиях, сигналы граждан, а также улучшить контроль за правильностью принимаемых должностными лицами дежурных частей решений.

В целях организации оперативного руководства патрульно-постовыми нарядами и обеспечения наблюдения за состоянием общественного порядка в местах массового сосредоточения людей находят применение средства телевизионной техники. Телевизионная техника используется и в интересах службы безопасности движения. Применяемая ***телевизионная аппаратура серии «Орбита»*** позволяет вести наблюдение за объектами, расположенными на расстоянии до 5 км от дежурной части, работает в интервале температур от –50 до +40 °С при номинальной освещенности на объектах до 20 люкс.

В помещениях дежурной части монтируются пульт-стол оператора и видеотерминальные устройства; внутри пульта управления размещаются блоки каналов, распределительно-коммутирующее устройство, блок питания, радиостанция.

С помощью телевидения осуществляется наблюдение за процессами, быстро изменяющимися во времени, когда информация, получаемая в результате использования обычных средств связи, не дает достаточного запаса времени для принятия соответствующих решений. Оно позволяет контролировать одновременно несколько объектов. Кроме того, создается возможность для коллективного наблюдения, чем исключается субъективность оценки обстановки.

Имеющаяся возможность изменения масштаба изображения позволяет на экране видеоконтрольного устройства отчетливо фиксировать знаки транспортных средств и другие предметы.

В качестве перспективных средств телевизионной техники для использования в работе дежурных частей можно отметить следующие:

– анализаторы телевизионных изображений, позволяющие получать информацию о состоянии охраняемых помещений, территорий;

– аппаратуру покадровой передачи телевизионного изображения по узкополосной кабельной (проводной) линии связи;

– подвижные специализированные телевизионные комплексы, осуществляющие прием-передачу видеоинформации по радиоканалу.

§ 2. Задачи, решаемые с помощью автоматизированных информационно-управляющих систем дежурных частей

В комплекс средств автоматизации дежурной части входят: оперативно-технические средства, размещаемые в дежурной части ОВД (зал дежурного, его помощников, зал службы «02» и радиоцентра), основными из которых являются автоматизированные рабочие места, оснащенные персональными ЭВМ (ПЭВМ), дисплеями и мониторами, светопланы коллективного пользования, средства связи и документирования; технические средства, размещаемые в технологических помещениях дежурной части, к которым относятся вычислительный комплекс, центр телекодовой связи, рабочие места технологического контроля системы и другие средства математического обеспечения.

Автоматизированная информационно-управляющая система дежурной части обеспечивает:

1. Анализ оперативной обстановки и выдачу на основе этого вариантов решений, направленных на оперативное реагирование по расследованию или предотвращению происшествий и обеспечивающих рациональное использование сил и средств.

2. Доведение до управляемых объектов, в том числе до экипажей патрульных нарядов и оперативных групп команд и целеуказаний, а также централизованный контроль за получением и ходом выполнения этих команд.

3. Сбор, обработку, документирование и отображение на средствах коллективного и индивидуального пользования информации об оперативной обстановке (о фактах происшествий) (например, в Москве — до 10 тыс./сут.), о расстановке сил и средств, местоположении патрульных нарядов, маршрутах их движения и т. д.).

4. Выдачу руководству информации об оперативной обстановке, отчетных документов и справок о результатах деятельности подчиненных подразделений за смену (или требуемый отчетный период) и другой информации.

5. Оперативный ввод в действие спецпланов («Перехват», «Вулкан» и др.) и контроль за ходом их выполнения.

6. Обмен информацией и взаимодействие между подразделениями и дежурными частями.

Комплексное применение средств автоматизации в деятельности дежурных частей открывает новые оперативные возможности повышения эффективности и качества выполнения задач, стоящих перед ОВД по охране общественного порядка и борьбе с преступностью.

Практика создания подобных автоматизированных систем в ряде УВД позволяет отметить следующие преимущества системы автоматизации деятельности дежурных частей по отношению к традиционным способам работы:

– исключается многоступенчатость в передаче исполнителю информации о происшествии с момента ее поступления в дежурную часть;

– поиск ближайшего свободного патрульного наряда осуществляется без участия человека;

– используется быстродействующая связь для передачи информации экипажам патрульных нарядов и в подразделения;

– отсутствует необходимость многократного на разных уровнях документирования информации по происшествию;

– обеспечивается автоматизация получения отчетных документов.

Все это сокращает время оперативного реагирования на факт правонарушения в 2–3 раза, что, в свою очередь, позволит повысить раскрываемость преступлений «по горячим следам».

Уровень информационного обеспечения сотрудников ОВД значительно повышается за счет организации прямого доступа к существующим информационным массивам ИВЦ и оперативного получения из них информации.

В общем виде имеется два пути решения проблемы создания в системе МВД РФ сети телеобработки данных с использованием ОВЧ-радиоканала:

– первый путь заключается в создании принципиально новой цифровой системы подвижной радиосвязи. И такое решение предполагает кардинальное перевооружение ОВД средствами радиосвязи, переход от аппаратуры с частотным разделением каналов к более совершенной — с кодовым разделением. Потребуются значительные финансовые затраты на разработку и промышленное производство необходимого количества новой техники;

– второй путь состоит в создании системы сбора и обработки данных на базе используемых в настоящее время стандартных ОВЧ-радиостанций, работающих в режиме данных или передачи телефонного сообщения; для этого могут быть использованы радиостанции комплексов «Виола». В этом случае имеется возможность создания сети обмена данными, работающей в режиме свободного доступа. То есть каждый абонент может связаться с любым абонентом этой сети.

Технически такой подход может быть выполнен путем подключения к низкочастотным входам радиосредств аппаратуры и устройств телеобработки данных, представляющих собой «интеллигентный» радиотерминал, портативный радиотерминал и радиомодем. Максимальное количество абонентов сети обмена данными для радиосистем с частотным разделением каналов равно 32.

В этом случае потребитель получает возможность передачи и чтения информации от любого абонента сети, а в режиме телефонии сохраняется возможность ведения разговора.

Доступность, простота и экономичность реализации при соблюдении оперативно-технических требований к системе передачи сообщений подтверждают правильность выбранного решения по созданию такой системы, ее перспективность.

Применение аппаратуры передачи данных в ОВЧ-радиосвязи позволит повысить оперативность реагирования подразделений и служб ОВД.

В ряде случаев такая связь может рассматриваться как единственно возможная для приема и передачи информации в условиях конспиративной работы. Одновременное документирование (протоколирование) процесса обмена информацией между дежурной частью и подчиненными подразделениями является новым направлением в деле совершенствования существующей системы управления и наиболее экономичным способом получения документальных данных о действиях ОВД при выполнении служебных задач.

При решении вопросов автоматизации деятельности дежурных частей важную роль играют устройства отображения информации коллективного пользования, выполняемые в виде светопланов или панно мозаичного типа. Такие устройства изготовляются индивидуально для каждого ОВД. Однако каждое из этих устройств содержит необходимую дежурной службе информацию об оперативной обстановке на обслуживаемой территории и размещении сил и средств с привязкой к картам-схемам региона. Перспективным направлением является применение слайдирования оперативных планов действий органов при изменениях обстановки. Использование ЭВМ для целей информационного обеспечения деятельности де-

журных частей позволяет высвечивать на экране дисплея и на проекционном табло оперативную обстановку, корректировать исходные данные для подготовки вариантов решений и указаний, контролировать визуально прохождение команд в реальном масштабе времени.

Разрабатываемые для дежурных частей ряда МВД, УВД устройства отображения информации коллективного пользования содержат технические решения на световодной технике, жидких кристаллах.

§ 3. Технологии функционирования дежурной части в условиях комплексного применения технических средств

В целях получения более полного представления о комплексном применении технических средств в деятельности дежурных частей рассмотрим технологию ее функционирования.

Основной поток информации о происшествиях в дежурную часть ОВД поступает через службу «02» по телефонным каналам. Оператор службы «02», определив характер происшествия и необходимость вмешательства полиции, оказывает помощь выдачей определенных рекомендаций либо коммутирует абонента на соответствующие службы, в том числе справочную. Телефонные линии «02» подключены к многоканальному магнитофону, с помощью которого ведется автоматическая запись переговоров. После регистрации информации оператор передает ее по телефону дежурному по ОВД и его помощнику, оператору радиоцентра (при необходимости вызова автомашин патрульных нарядов, оперативных групп), дежурным по подчиненным органам, на территории которых произошло происшествие.

В автоматизированных информационно-управляющих системах сведения о происшествиях вводятся в диалоговом режиме с клавиатуры дисплея ЭВМ путем заполнения высвечиваемого на экране бланка.

При этом автоматизированная система обеспечивает проведение операций по регистрации происшествия, определению состава и количества сил и средств, необходимых для реагирования; определяет ОВД, на территории которого произошло происшествие.

После принятия решения дежурный оператор радиоцентра дежурной части по радиоканалам передает задания экипажам патрульных нарядов, находящихся в районе происшествия.

Телефонные и телеграфные каналы связи дежурной части используются для организации обмена информации с подчиненными и взаимодействующими ОВД, вышестоящим органом, руководством данного ОВД. Технические средства оповещения личного состава применяются при введении специальных планов.

Для выезда к месту происшествия оперативных групп в дежурных частях имеются специальные автомобили, приспособленные и укомплектованные необходимыми техническими средствами для осмотра места происшествия, проведения операций по захвату вооруженных преступников и другими средствами.

Организация работы дежурных частей различного уровня производится в соответствии с инструкциями, объявленными нормативными актами МВД РФ. В этих инструкциях и приказах, кроме выполнения управленческих функций, поставлена задача твердого усвоения работниками дежурных частей порядка эксплуатации, сбережения и умелого применения на практике технических средств, находящихся в их распоряжении.

Тема 14. СРЕДСТВА УСИЛЕНИЯ РЕЧИ

§ 1. Назначение и основные направления применения средств усиления речи в оперативно-служебной деятельности

Средства усиления речи, используемые в ОВД, являются локальными средствами массовой информации. Они могут использоваться как для внутренних целей, т. е. для информации соответствующих подразделений и отдельных сотрудников ОВД, так и внешних — для передачи информации гражданам, отдельным правонарушителям и т. п. Они находят применение не только в работе территориальных ОВД, но и в деятельности ИТУ.

Средства усиления речи (СУР) используются для управления силами и средствами подразделений при проведении различных мероприятий оперативно-служебного характера, построений, проведения учений, для оповещения и т. п. При использовании средств усиления речи информацию следует передавать четко, грамотно и лаконично, соблюдать нормативно-уставные требования.

Большое значение имеет применение СУР при профилактике нарушений правопорядка в общественных местах (на улицах, в местах отдыха граждан и др.). Широкое применение они нашли в деятельности ГИБДД (при регулировании и обеспечении безопасности движения транспорта и пешеходов).

Кроме того, СУР используются сотрудниками ОВД с целью обеспечения порядка при проведении различных массовых мероприятий.

Указанные средства также могут использоваться для передачи гражданам различной информации. В частности, они могут применяться в приемных паспортных столов для передачи справочной информации, а также информации, носящей профилактический характер (предупреждение краж, побегов, пожаров и т. п.).

СУР успешно используются в сочетании с другими техническими средствами, применяемыми в оперативно-служебной деятельности. Так, при проведении оперативно-розыскных мероприятий по задержанию преступников они используются вместе с приборами видения в темноте, средствами связи и транспортом. Согласно нормативным требованиям эти средства необходимо использовать для предупреждения преступников перед применением средств типа «Черемуха». Положительные результаты дает использование средств усиления речи в комплексе со средствами телевизионного обзора, применяемыми в дежурных частях ОВД и ИТУ. При передаче часто повторяющейся информации к СУР подключается звукозаписывающая аппаратура с заранее подготовленной записью нужного текста.

Таким образом, масштаб использования СУР достаточно широк. При успешном применении они являются мощным средством для поддержания правопорядка и борьбы с преступностью. Необходимо отметить, что использование СУР требует достаточно высокой подготовки личного состава.

Прежде всего следует иметь в виду, что неисправность этих средств в ряде случаев может привести к срыву проводимых мероприятий. Поэтому требуется тщательный контроль за их техническим состоянием и, особенно, за состоянием блоков питания. При использовании СУР нужно обращать внимание на

правильное их расположение, учитывать расстояние до получателя информации, направление ветра, наличие вблизи поверхностей, отражающих звук (стены, заборы и т. п.).

§ 2. Виды средств усиления речи, их классификация

Средства усиления речи в зависимости от назначения подразделяются на носимые, мобильные, стационарные.

Носимые СУР (электромегафоны) применяются при проведении массовых мероприятий, в ходе операций по задержанию вооруженных преступников для убеждения их отказаться от сопротивления, а также для управления действиями личного состава.

Мобильные СУР (громкоговорящие установки) монтируются на различных транспортных средствах и используются для указанных выше целей, а также при преследовании задерживаемых, при обеспечении сопровождения спецтранспорта, в агитационных целях (например, по линии ГИБДД).

Стационарные СУР (трансляционные усилители) устанавливают внутри зданий ОВД для оповещения личного состава, а также на объектах ИТУ в целях подачи команд осужденным, проведения воспитательной работы.

В основу работы СУР положен принцип преобразования звуковых колебаний с помощью микрофона в слабый электрический ток с последующим его усилением и обратным преобразованием в звуковые колебания посредством динамического громкоговорителя.

Основными частями носимых СУР являются: микрофон, усилитель, электродинамический громкоговоритель с рупором, источник питания, устройство включения.

Микрофон служит для преобразования звуковых колебаний воздуха в электромагнитные.

Колебания воздуха воздействуют на диафрагму микрофона и приводят ее в движение. Так как диафрагма микрофона колеблется между наконечниками магнитной системы, то магнитный поток, проходящий между ними, изменяется в такт этим колебаниям. Это приводит к индуктированию в катушках микрофона напряжения звуковой частоты, соответствующих звуковым колебаниям воздуха возле микрофона.

Конструкция применяемых микрофонов такова, что они обладают высокой шумостойкостью, т. е. не воспринимают звуковых колебаний, идущих от удаленных источников звука. Вследствие этого для обеспечения нормальной работы средств усиления речи необходимо, чтобы микрофон находился на расстоянии 1–2 см от угла рта оператора, а при использовании мобильных и стационарных усилителей речи — на расстоянии 20–30 см.

Усилитель низкой частоты электромегафона предназначен для усиления напряжения, развиваемого микрофоном, до уровня, обеспечивающего получение на выходе необходимой мощности.

Электродинамический громкоговоритель предназначен для преобразования электрических колебаний и акустическую отдачу громкоговорителя и создает направленное излучение. Звуковая катушка громкоговорителя тесно связана с мембраной. Вследствие этого при прохождении через катушку тока звуковой частоты мембрана колеблется с такой же частотой и вызывает колебания прилегающего

к ней слоя воздуха. Далее колебания воздуха распространяются по рупору и направленно излучаются в окружающее воздушное пространство.

Источниками питания носимых средств усиления речи могут быть батареи, используемые для карманного фонаря, гальванические элементы 316, 336, 373, аккумуляторы типа ЦНК-0,45 и т. п. В некоторых случаях могут использоваться и внешние источники питания.

Устройство включения электромегафона выполняется обычно в виде кнопки, расположенной на рукоятке. Нажатием кнопки производится включение питания на усилитель.

Мобильные СУР состоят из тех же основных частей, что и носимые. Вместе с тем вследствие специфики их применения они имеют и некоторые дополнительные элементы. К ним в первую очередь необходимо отнести устройства для крепления этих средств на соответствующие подвижные объекты, позволяющие осуществлять повороты громкоговорителей. Кроме того, мобильные СУР имеют устройства, обеспечивающие регулировку громкости и тембра звука, а также подключение магнитофона, звукоснимателя и т. п. В ряде случаев эти средства комплектуются и ларингофонами.

Стационарные средства усиления речи по составу аппаратуры практически состоят из тех же элементов, что и рассмотренные выше. В отличие от носимых и мобильных в них используются более мощные усилители. Электропитание стационарных СУР осуществляется в основном от сети 220 В 50 Гц.

Основные тактико-технические данные средств усиления речи приведены в таблице 14.2.1.

Таблица 14.2.1 — Основные тактико-технические данные средств усиления речи

Технические характеристики	----- ЭМ-2|	Наименование СУР ЭМ-7 | ЭМ-12 | 5ПЭМ-1 | ГУ-20	СГУ-60
Мощность на выходе усилителя не менее, ВТ	4	8 | 12 | 5 | 10 × 2	60
Номинальное напряжение питания, В	12	8,5 | 16 | 10 | 12	12
Время непрерывной работы от одного комплекта батарей не менее, ч	1,5	1,5 | 10 | 1,5 | –	–
Масса с источником питания не более, кг	2,8	3 | 2,4 | 1,9 | 20	20

§ 3. Тактические особенности использования средств усиления речи

Средствами усиления речи в соответствии с нормами табельной положенности ОВД (Приказ МВД России от 20 мая 1993 г. № 036) обеспечиваются патрульно-постовая служба, подразделения ГИБДД, аппараты ИТУ, дежурные части и др.

Выбор того или иного типа СУР зависит от конкретной цели и условий их использования. Так, для воздушного патрулирования при наличии большого шума собственных двигателей и движущегося наземного транспорта, на вертолетах устанавливаются звукоусиливающие станции мощностью до 500 Вт; для обеспечения работы наземного транспорта ГИБДД используются усилители речи меньшей мощностью (***СГУ-60; ГУ-20; ГУ-10*** и др.).

При передаче речи в больших закрытых помещениях (стадионах, спортивных залах, станциях метро и т. д.) целесообразно использовать носимые электромегафоны ***«5ПЭМ-1»*** или ***«ЭМ-2м».***

Следует учитывать, что на открытых участках местности эти мегафоны обеспечивают направленную передачу команд и распоряжений соответственно до 150 и 300 м лишь при благоприятных условиях: отсутствие ветра, направление ветра в сторону передачи, сравнительно небольшие производственные шумы и т. д.

При неблагоприятных условиях на открытой местности целесообразно использовать более мощные усилители речи (например, СГУ-60).

Усилители речи являются мощным средством психологического воздействия. Усиленный голос оператора перекрывает посторонние отвлекающие шумы, сосредоточивает внимание людей, к которым обращена речь, на содержащейся в ней информации. На эту речь невольно обращают внимание и все остальные люди, в том числе и проживающие в близко расположенных домах, либо работающие в рядом находящихся учреждениях.

В связи с этим нельзя злоупотреблять средствами усиления речи: их используют только в тех случаях, когда обычный голос или иной сигнал не воспринимается адресатом.

Средства усиления речи используются при необходимости:

– остановить движение транспортных средств, колонны людей или изменить их направление, когда другими средствами сделать это затруднительно;

– предупредить нарушителя правил движения, а также пешехода или водителя транспортного средства о какой-либо возможной опасности;

– потребовать удалиться посторонних лиц с места происшествия в целях сохранения следов преступления;

– напомнить гражданам о необходимости соблюдать порядок в той или иной обстановке;

– потребовать от преступника, укрывшегося в помещении, прекратить стрельбу, сложить оружие и сдаться.

Перечисленные случаи не являются исчерпывающими в повседневной деятельности ОВД. Однако при всем их разнообразии требуется соблюдение условий, без которых применение средств усиления речи может оказаться неэффективным либо привести к отрицательным последствиям.

К этим условиям относятся:

– четкое указание адресата, к которому обращена речь. Для этого используются, например, признаки одежды («Гражданин в черном костюме...»), номер транспортного средства («Водитель такси №...»), количество лиц и их возраст («Молодые люди...») и другие;

– краткость и логичность речи. В ней должна содержаться сущность передаваемой информации, речь должна быть простой и понятной;

– законность и обоснованность содержащегося в обращении требования. В необходимых случаях следует объяснить, в связи с чем это требование предъявляется. Например: «Граждане! Не переходите зону ограждения! Эта зона находится под обстрелом вооруженного преступника». Или: «Граждане! В целях сохранения следов преступника прошу всех удалиться за зону ограждения!»;

– соблюдение вежливости обращения. Недопустимы окрики, унижающие достоинство граждан, развязность, раздраженность и грубый тон, вызывающие справедливое возмущение окружающих и дискредитирующие ОВД;

– категоричность требования. При необходимости обращение следует повторить несколько раз, через определенные промежутки времени. Во всех случаях окружающим гражданам должна быть понятна необходимость использования средств усиления речи;

– использование уровня громкости, достаточной лишь для достижения цели, но не более. Необходимо при этом избегать появления акустической завязки, вызывающей у окружающих слуховые ощущения.

Стационарные усилители речи устанавливаются в дежурных частях ОВД и используются для оповещения и вызова оперативных групп для выезда на место происшествия, передачи циркулярных команд всему личному составу и т. д.

В ГИБДД стационарные усилители речи используются при проведении агитационно-массовой и пропагандистской работы. Широкое применение стационарные усилители речи находят в деятельности ИТУ. Они устанавливаются как по периметру ИТК, так и внутри колонии (в жилых помещениях, в пром. зоне и т. п.).

Пример обращения к вооруженному преступнику Осипову с требованием сложить оружие и сдаться:

«Осужденный Осипов! С вами говорит начальник ИТК-10 полковник Кравцов. Предлагаю немедленно прекратить стрельбу, отпустить заложников и сдаться! Сопротивление бесполезно: все выходы из помещения блокированы. Подумайте о себе и своих детях. Еще не поздно. Предупреждаю: ровно через пять минут, если не одумаетесь, к вам будут приняты самые решительные меры со всеми вытекающими последствиями! Осипов! Осталось две минуты для вашего размышления. Еще не поздно бросить оружие и добровольно сдаться — только это может облегчить вашу участь!»

Список использованной литературы

1. Конституция Российской Федерации от 12 декабря 1993 г. (в ред. от 21 июля 2014 г.) [Текст] // СЗ РФ. — 2009. — № 4. — Ст. 445.
2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 31.12.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
3. «Уголовно-исполнительный кодекс Российской Федерации» от 08.01.1997 № 1-ФЗ (ред. от 20.12.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_12940/
4. Закон Российской Федерации от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» (ред. от 05.12.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_385/
5. Закон Российской Федерации от 21.07.1993 № 5473-1 «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» (ред. от 28.12.2016) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_4645/
6. Федеральный закон Российской Федерации от 15.07.1995 № 103-ФЗ «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений» (ред. от 28.12.2016) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_7270/
7. Федеральный закон Российской Федерации от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности в Российской Федерации» (ред. от 06.07.2016) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_7519/
8. Федеральный закон Российской Федерации от 21.07.1997 № 118-ФЗ «О судебных приставах» (ред. от 29.12.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_15281/
9. Федеральный закон Российской Федерации от 27.12.2002 № 184-ФЗ «О техническом регулировании» (ред. от 27.07.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_40241/
10. Федеральный закон Российской Федерации «О связи» от 07.07.2003 № 126-ФЗ (ред. от 05.12.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_43224/
11. Федеральный закон Российской Федерации «О полиции» от 07.02.2011 № 3-ФЗ (ред. 05.12.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_110165/
12. Федеральный закон Российской Федерации от 03.07.2016 № 226-ФЗ «О войсках национальной гвардии Российской Федерации» (ред. от 05.12.2017) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_200506/
13. Указ Президента Российской Федерации от 18.09.1993 № 1390 «О дополнительных мерах по укреплению правопорядка в Российской Федерации» [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_356/
14. Указ Президента Российской Федерации от 08.10.1997 № 1100 «О реформировании уголовно-исполнительной системы МВД РФ» [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_16395/
15. Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_191669/

16. Приказ Министерства внутренних дел Российской Федерации от 11.09.1993 № 423 «Об утверждении Инструкции о порядке применения химических ловушек в раскрытии краж имущества, находящегося в государственной, муниципальной, частной собственности и собственности общественных объединений (организаций)» [Электронный ресурс]. — URL: http://base.garant.ru/1305831/

17. Приказ Министерства внутренних дел Российской Федерации от 16.08.2003 № 647 «Об утверждении наставления по эксплуатации технических средств подразделениями вневедомственной охраны при органах внутренних дел». [Электронный ресурс]. — URL: https://normativ.kontur.ru/document?moduleId=1&documentId=69958

18. Приказ Министерства юстиции Российской Федерации от 13.09.2005 № 759 «Об утверждении норм положености и нормативных сроков эксплуатации инженерно-технических средств охраны и надзора, норм расхода запасных частей и эксплуатации, норм положености электротехнического оборудования и средств защиты для территориальных органов, учреждений и подразделений уголовно-исполнительной системы ФСИН России» (ред. от 25.08.2008) [Электронный ресурс]. — URL: http://base.garant.ru/1356884/

19. Приказ Министерства юстиции Российской Федерации от 04.09.2006 № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы» [Электронный ресурс]. — URL: http://base.garant.ru/57742441/

20. Приказ Федеральной службы исполнения наказания Российской Федерации от 03.03.2005 № 38 «Об утверждении Перечня инженерно-технических средств охраны и надзора для органов и учреждений Федеральной службы исполнения наказаний» [Электронный ресурс]. — URL: http://фсин.рф/document/

21. Приказ Федеральной службы исполнения наказания Российской Федерации от 14.03.2005 № 93 «Об утверждении Руководства по определению категорий оборудования комплексом инженерно-технических средств охраны и надзора объектов уголовно-исполнительной системы» [Электронный ресурс]. — URL: http://фсин.рф/document/

22. Приказ Федеральной службы исполнения наказания Российской Федерации от 18.08.2006 № 574 «Об утверждении Руководства по технической эксплуатации инженерно-технических средств охраны и надзора, применяемых для оборудования объектов уголовно-исполнительной системы» [Электронный ресурс]. — URL: http://фсин.рф/document/

23. Приказ Федеральной службы исполнения наказания от 05.12.2014 № 233 «Об утверждении инструкции о подготовке уголовно-исполнительной системы действий при чрезвычайных обстоятельствах» [Электронный ресурс]. — URL: http://фсин.рф/document/

24. Инструкция Федеральной службы исполнения наказания от 15.02.2006 № 21 «Об утверждении инструкции по охране исправительных учреждений, следственных изоляторов уголовно-исполнительной системы» [Электронный ресурс]. — URL: http://фсин.рф/document/

25. *Бузов, Г. А.* Защита от утечки информации по техническим каналам: учеб. пособие для подготовки экспертов системы Гостехкомиссии России [Текст] / *Г. А. Бузов, С. В. Калинин, А. В. Кондратьев*. — М. : Горячая линия — Телеком, 2005. — 416 с.

26. *Дорогин, Д. А.* Применение оружия при исполнении обязанностей караульной службы как обстоятельство, исключающее уголовную ответственность [Текст] / *Дорогин Д. А.* // Военно-юридический журнал. — 2015. — № 12.

27. *Конеев, И. Р.* Информационная безопасность предприятия [Текст] / *И. Р. Конеев.* — СПб. : БХВ Петербург, 2003. — 752 с.

28. *Куракин, А. В.* Правовое регулирование применения полицией дистанционно управляемого вооружения [Текст] / *А. В. Куракин, А. Ю. Молянов, Д. А. Митюшин, А. Н. Харитонов* // Современное право. — 2017. — № 4.

29. *Попов, В. Г.* Специальная техника, применяемая в УИС России : учеб. пособие для дополнительного профессионального образования сотрудников УИС России [Текст] / *В. Г. Попов* : В 2 ч. — Томск : Томский филиал ФГОУ ВПО «Кузбасский юридический институт ФСИН России», 2008. — 240 с.

30. *Попов, В. Г.* Использование систем видеонаблюдения и кабельного телевидения при осуществлении надзора за осужденными: учеб. пособие [Текст] / *В. Г. Попов.* — Томск : Томский филиал Академии права и управления ФСИН России, 2005. — 71 с.

31. *Попов, В. Г* Информационная техника и технологии, применяемые в УИС : учеб. пособие для среднего специального, высшего и дополнительного профессионального образования сотрудников ФСИН России [Текст] / *В. Г. Попов.* — Томск : Томский филиал Академии права и управления ФСИН России, 2007. — 171 с.

32. *Свининых, Е. А.* Статья: О правовых режимах закупок товаров, работ, услуг для обеспечения обороны страны и безопасности государства [Текст] / *Е. А. Свининых* // Право в Вооруженных Силах. — 2015. — № 12.

33. *Скобелин, С. Ю.* Использование специальных знаний при работе с электронными следами [Текст] / *Скобелин С. Ю.* // Российский следователь. — 2014. — № 20.

34. *Хорошко, В. А.* Методы и средства защиты информации (под редакцией Ковтанюка) [Текст] / *Хорошко В. А., Чекатков А. А.* — К. : Издательство Юниор, 2003. — 504 с.

35. *Ярочкин, В. И.* Информационная безопасность : учебник для студентов вузов [Текст] / *В. И. Ярочкин.* — 3-е изд. — М. : Академический проект: Трикста, 2005. — 544 с.

Учебное издание

Составители:
Пудаков Евгений Рустамович
Яппаров Роман Рауфович

СПЕЦИАЛЬНАЯ ТЕХНИКА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Учебное пособие

Компьютерная верстка Бурмистровой А. Г.
Техническое редактирование: Бочарова Т. Е.

Сдано в набор 20.11.2017. Подписано в печать 22.12.2017.
Формат 60 × 84/16. Бумага офсетная. Печать ризографическая.
Усл. печ. л. 16,74. Уч.-изд. л. 17,35. Тираж 300. Заказ 124

Башкирский институт социальных технологий (филиал)
Образовательного учреждения профсоюзов высшего образования
«Академия труда и социальных отношений»

450054, г. Уфа, проспект Октября, 74/2.
Тел.: +7 (347) 241-42-59.
www.ufabist.ru

Отпечатано в типографии БИСТ (филиала) ОУП ВО «АТиСО»