**Введение.**

Человек всегда стремился знать как можно больше о соседях. В нашу постиндустриальную эру информация приобрела решающую роль.
В большинстве индустриально развитых стран информация является первоосновой всех аспектов развития общества. Преимущество и специфика информации заключается в том, что она не исчезает при потреблении, не передается полностью при обмене (оставаясь в информационной системе и у пользователя), является "неделимой", т. е. имеет смысл только при достаточно полном наборе сведений, что качество ее повышается с добавлением новой информации. Действительно, общество, научно-техническая, производственно-практическая, теоретическая деятельность которого основана на оперативно накапливаемой, разумно используемой информации, в принципе получает в свое распоряжение ресурсы огромной значимости, доступные многократному и многостороннему использованию, дальнейшему "возобновлению" в усовершенствованном виде и быстрому созданию новых информационных систем.

Информация - это, во-первых, знание относительно нового типа, пригодное для дальнейшего использования, а, во-вторых, знание, производство, хранение и применение которого действительно становится все более важной для общества деятельностью, порождает соответствующие ему технико-организационные структуры [1].

К 400 году до н.э. Восток значительно опередил Запад в искусстве разведки. Сунь Цзы писал: "То, что называют предвидением, не может быть получено ни от духов, ни от богов...ни посредством расчетов. Оно должно быть добыто от людей, знакомых с положением противника" [2].
С этого начался несанкционированный доступ к информации (НДкИ). Очень преуспели в нем многие государи и частные лица. Прекрасно поставленная служба разведки помогала купцам Венеции и банкирскому дому Фуггеров, фирме Круппа и дому Ротшильдов. Методы практически не менялись столетиями: подкупали, шантажировали, посылали послов-шпионов, перехватывали письма, читали пергаменты (позже книги и газеты) в библиотеках и монастырях. Когда удавалось, подсматривали и подслушивали. Трудности возникали и тогда: надо было передавать полученную информацию в центр сбора и обработки. Для этого приходилось гнать не всегда надежных гонцов, лично пробегать марафонскую дистанцию или пользоваться голубиной почтой. А чтобы не забыть по дороге, о чем шла речь, содержание перехваченных переговоров записывали, а иногда и шифровали.

Таким образом, мы видим прообраз технической системы съема информации:

* микрофон, фотоаппарат, камера - ухо или глаза шпиона;
* диктофон или система накопления информации - записки;
* радиоканал, провода и т.д. - гонец;
* приемник - лицо, принявшее сообщение у гонца.

Что касается анализа полученной информации, то все осталось без изменений нужен человек или группа людей, умеющих думать. Единственно, их работу сейчас несколько облегчила вычислительная машина.
 Развитие техники вплоть до начала ХХ века не влияло на средства несанкционированного съема информации: сверлили дырки в стенах и потолках, использовали потайные ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появление телеграфа и телефона позволило использовать технические средства получения информации. Гигантское количество сообщений стало перехватываться, влияя на ведение войн и положение на бирже. В 30-40 годы появились диктофоны, действительно миниатюрные фотоаппараты и различные радиомикрофоны. В дальнейшем все большее значение приобретал перехват данных, обрабатываемых в компьютерах, но совершенствовались и традиционные средства.

Целью данной курсовой работы является ознакомление курсантов с некоторыми методами и средствами получения информации, которые реально используются или могут быть использованы в ближайшее время.

**1 Методы, применяемые для НДиК**

Сбор сведений ведется самыми различными способами, причем большинство из них не являются таинственными или секретными. Это относится, в первую очередь, к открытым сведениям, то есть информации, почерпнутой из газет, книг, научных и технических изданий, официальных отчетов и рекламных материалов. Подобным образом работает большинство разведок мира. Такая деятельность ведется широко и основательно, при этом нужно не упустить ничего, что доступно и что могло бы оказаться полезным. Понятно, что для анализа требуется группа аналитиков.

Перечислим некоторые методы по которым может производиться НДиК:

• прослушивание телефонных аппаратов

• дистанционное звуковое прослушивание

• доступ к компьютерным банкам данных

• копирование носителей информации

• расшифровка радиоизлучения компьютеров, факсов, телетайпов

• слуховой контроль через резонирующие перегородки, стёкла, стены, батареи отопления.

• установка микропередатчиков в помещениях, автомобилях

• использование эффекта индуктивности любых неэкранированных проводников внутри помещений (линий связи, электропитание, сигнализация).

**2 Параметры и технические средства для НДиК**

Далее будут рассмотрены средства НДиК и параметры по которым осуществляется съем информации.

**2.1 Акустические сигналы**

Звуковыми или акустическими сигналами называются распространяющиеся в упругой среде механические колебания с малыми амплитудами.

**2.1.1 Микрофоны**

***A. Передача информации по специально проложенным проводам***

Простейшей и наиболее надежной операцией является использование специального малогабаритного микрофона (размером 7x5x2 мм) и специально проложенного провода. Она заключается в том, что скрытно размещенный в интересующем помещении микрофон соединяется с пунктом прослушивания, где перехваченные разговоры записываются через усилитель на магнитофон либо прослушиваются. До появления микроэлектроники описанный способ применялся чрезвычайно широко.
Недостатком проводов является возможность их обнаружения и проверки назначения при визуально-техническом контроле. В более современных системах используются тончайшие (не толще волоса) оптические волокна, которые возможно вплести в ковровое покрытие, и т.д. Разумеется, микрофон в его привычном понимании отсутствует.
Несмотря на видимую простоту, специалисты не очень любят подобные средства, поскольку по проводу можно обнаружить пункт прослушивания, со всеми вытекающими отсюда неприятными последствиями.

***Б. Использование имеющихся коммуникаций***

Гораздо более безопасным является использование выходящих за пределы помещения проводов сигнализации, радиотрансляции и т.д., а также металлоконструкций типа труб системы отопления, канализации, водоснабжения. Микрофон с предусилителем, скрытно установленный в интересующем помещении, подключается к подобным конструкциям, с которых информация снимается в пункте прослушивания. В данном случае требуется более совершенная аппаратура как для передачи, так и для приема акустических сигналов. В качестве примера можно привести систему ЛСТ-ОС-1, микрофон которой размещен в датчике охранной сигнализации, устанавливаемом на объекте. Система ЛСТ-ВО-2 позволяет осуществлять передачу перехваченной информации по трубам парового отопления и другим металлоконструкциям [15].

***В. Использование сети 220 Вольт***

Очень популярным средством съема информации являются системы, устанавливаемые в электророзетках, выключателях и т.д., передающие разговоры по проводам 220 В. Этот способ очень удобен для включения и выключения передатчика, который имеет неограниченный источник энергопитания, но в данном случае осложняется вопрос размещения постов прослушивания, так как передаваемые по электропроводам сигналы не проходят через силовые трансформаторы. Диапазон частот используемых сигналов - от 50 кГц до 300 кГц. При меньших значениях будут сильно сказываться сетевые низкочастотные помехи, а при больших значениях резко возрастает затухание в проводах, а также начинает усиливаться электромагнитное излучение, которое сводит на нет все преимущества по скрытности.

***Г. Передача информации по телефонным линиям***

Широкое распространение в последнее десятилетие получили системы акустического прослушивания помещений через телефонную линию. Рассмотрим алгоритм работы подобных систем на примере TELE-MONITOR [16]. На телефонной линии (внутри телефонного аппарата) устанавливаются специальные датчики (подключаются параллельно). При необходимости прослушать разговор производится звонок с любого телефона, в том числе и по междугородней связи, и выдается в телефонную трубку специальный сигнал. Звонки в этом случае не проходят на телефон и датчик TELE-MONITOR начинает передавать в линию разговоры, происходящие в помещении. Таких датчиков можно установить до четырех, скажем, для контролирования четырех комнат квартиры, при этом инициировать их в любой последовательности.
Главным их недостатком является то, что либо звонок проходит на телефон, либо необходимо делать два звонка.
 ***Д. Радиотелефоны***

Радиотелефоны или радиозакладки занимают лидирующее место среди используемых средств технического съема информации. Простейшее устройство содержит три основных узла, определяющих технические возможности и методы их использования, - микрофон, определяющий зону акустической чувствительности, радиопередатчик, определяющий дальность ее действия, источник питания, от которого зависит продолжительность ее непрерывной работы. На дальность и качество оказывают влияние также и характеристики приемников.

В мире существуют тысячи разновидностей радиомикрофонов. Можно привести следующие обобщенные данные по отечественных и импортным закладкам, предлагаемым сегодня на рынке:

* диапазон:, 30...1300 МГц
* мощность:, 0, 2...500 мВт
* ток потребления:, 0, 5...100 мА
* дальность действия:, 10...1500 м (без ретранслятора)
* период активного существования:, 4 часа...20 лет.

Как правило, во всех системах используется широкополосная ЧМ и только в некоторых - узкополосная. Большинство предлагаемых недорогих изделий не имеют кварцевой стабилизации, в ряде случаев это не нужно. Габариты колеблются от нескольких миллиметров до десятков сантиметров.
Для приема используются самые различные устройства: от бытовых магнитол до высокопрофессиональных устройств. Пожалуй, основной характеристикой системы "закладка-приемник" является чувствительность приемника. Чем лучше этот параметр, тем дальше то расстояние, на которое можно использовать эту систему.

Рассмотрим три типа используемых приемников.

К первому типу относятся обыкновенные бытовые приемники и магнитолы. Преимущество магнитол заключается в возможности записи информации, передаваемой по радиоканалу. К плюсам таких систем можно отнести их низкую стоимость и двойное назначение. К тому же они обычно не вызывают подозрение. К минусам относятся: низкая чувствительность, что ограничивает дальность применения; использование общедоступного радиодиапазона (для отечественных приемников 62- 74 МГц, для импортных - 88-108 МГц).
Частично эти недостатки устранены в приемниках второго типа. Обычно "поднимают" диапазон рабочих частот до 130 МГц у стандартных бытовых магнитол и пытаются несколько улучшить чувствительность. Добиваются этого, как правило, перестройкой контуров или применением конвертеров. В последнем случае частотный диапазон может выбираться практически любой.
Но это все полумеры. Профессионалы используют специально разработанную технику. В качестве примера рассмотрим приемник ЛСТ-П-3. Чувствительность его порядка 1, диапазон - 110...160 МГц [15]. Все органы управления выполнены на кнопках.
 Говоря о радиозакладках, нельзя обойти вниманием системы типа SIPE PS [7]. Это комплект, состоящий из бесшумного пистолета с прицельным расстоянием 25 м и "радиозакладки-стрелы". Предназначен для установки закладки в местах, физический доступ к которым невозможен. Стрела с миниатюрной радиозакладкой в ударопрочном исполнении надежно прикрепляется к поверхностям из любого материала - металла, дерева, пластмассы, камня, бетона и т.д. Микрофон обеспечивает съем речевой информации в радиусе до 10 м, а передатчик - ее трансляцию на расстояние до 100 м. Тактики применения следующая: "стрела" отстреливается через открытое окно и прикрепляется к стене. В реальных условиях города дальность не превышает 50 м и это обстоятельство резко снижает в ряде случаев оперативную ценность системы.
Как правило, лимитирующим фактором является питание. Из-за недолговечности батареек агенту требуется периодически проникать на объект, что сопряжено с риском.
Для увеличения времени функционирования стараются увеличить емкость батарей, но этот путь имеет пределы. Стараются увеличивать время работы путем установки источников питания больших размеров, если это возможно.
 Конструкторы спецтехники пошли по пути запитывания радиозакладок от внешних источников.
Одним из направлений стало использование собственного питания камуфляжа, т. е. изделий, в которых замаскирован радиомикрофон. В качестве примера можно привести установление в калькуляторе изделие ЛСТ-3. Габариты - 12x5x3 мм, чувствительность микрофона 10м, дальность передачи в диапазоне 112-135 МГц - 150 м. В качестве источника питания используется батарейка калькулятора. Если необходимо, поставляется ЛСТ-3 в комплекте с плоской (не толще 1. 5 мм) и гибкой литиевой батарейкой, что позволяет вшивать изделие в одежду, размещать в корешке книг и т.д.
Другим направлением является использование сети 220В. В качестве примера можно привести ЛСТ-4, которое устанавливается в электророзетках, настольных лампах и других электроприборах, благодаря чему имеет практически неограниченное время применения. Классическим образцом западной технической мысли является изделие HR560 LIGHT WULD [17]. Это передатчик, встроенный в цоколь обыкновенной лампочки накаливания с дальностью передачи до 250 м. Можно запитать радиомикрофон и напряжением телефонной линии, как это сделано в ЛСТ-3Т5 [17].
Третьим направлением является использование солнечных батареек. Пока подобные устройства не получили широкого распространения из-за ряда своих врожденных недостатков, а именно невозможности работать в условиях слабой освещенности. Пожалуй только изделие типа SIPE MT достойно описания. Это ЧМ-передатчик с питанием от солнечной батареи, выполненный в виде стакана для виски. Элементы солнечной батареи расположены на дне стакана в виде оригинального орнамента. Для повышения скрытности передатчик имеет два режима: он включен если стакан стоит на столе, и отключается если его поднять и изменить положение в пространстве. Дальность действия передатчика в диапазоне 130....150 МГц составляет 100 м [7].
Кроме того, экономить питание и повысить скрытность позволяет использование дистанционного включения. Таково изделие TRM-1530. Это радиозакладка со встроенным микрофоном и запитанное от 3-х литиевых батареек. Работает в диапазоне 100...150 МГц, габариты 87x54x20 мм, время непрерывной работы не менее 900 часов, а с учетом периодического выключения не менее 3600 часов. Дальность действия - 150 м. Интересным направлением является использование ретрансляторов. Подобная систем а состоит из двух частей: радиозакладки, габариты которой минимальны, и ретранслятора, габариты и питание которого практические не лимитированы. Суть дела такова. Дальность действия радиомикрофона не превышает 10...100 м, благодаря чему снижается ток потребления и, следовательно, возрастает время работы. Ретранслятор же устанавливается в соседнем помещении, автомобиле и т.д. Питаясь от стационарных источников, он обеспечивает передачу перехваченной информации на требуемую дальность. Появление изотопных батареек позволило резко увеличить время непрерывной работы радиозакладок. Так, ЛСТ-2-РБ с питанием от изотопного элемента в габаритах "кроны" может работать не менее 10 лет. Подобные устройства негосударственным органам и частным лицам не продаются. Такие радиомикрофоны находили в мраморных плитках внешней облицовки зданий, а также в кирпичах внутренней кладки зданий. В заключение хочется отметить что подобные изделия искать достаточно сложно. Так, в новом здании американского посольства элементы радиозакладок были "рассредоточены" по бетонным блокам, представляя собой кремневые вкрапления, арматура использовалась в качестве проводников, а пустоты - в качестве резонаторов и антенн [17].
 В заключение опишу самый маленький и самый дорогой в мире радиомикрофон, габариты которого не превышают четверти карандашной стирательной резинки. Этот миниатюрный передатчик питается от изотопного элемента и стоит порядка 40 тыс. $. Он способен в течение года воспринимать и передавать на приемное устройство, расположенное в полутора километрах, разговор который ведется в помещении шепотом. Кроме того, уже сейчас производятся "клопы", которые могут записывать перехваченную информацию, хранить ее в течении суток или недели, передать в режиме быстродействия за миллисекунду, стереть запись и начать процесс снова.

***Е. ИК-передатчики***

Для повышения скрытности, в последние годы стали использовать для передачи перехваченной микрофоном информации инфракрасный канал. В качестве передатчиков используются маломощные полупроводниковые лазеры и светодиоды. В качестве примера рассмотрим закладку TRM-1830. Дальность действия ее днем 150 м, ночью - 400 м. Ток потребления - 8 мА, время непрерывной работы - 20 часов. Габариты не превышают 26x22x20 мм. К недостаткам можно отнести необходимость прямой видимости между закладкой и приемником и влияние фоновой засветки. Все это резко ограничивает оперативные возможности подобных средств.

**2.1.2 Направленные микрофоны.**

Обычные микрофоны динамического или электретного типа способны регистрировать голос человека с нормальной громкостью на расстоянии до 15 метров, а ночью, в тихую погоду, - 200 м. Для средств разведки этого мало, так как в некоторых случаях требуется дальность действия примерно в десять раз больше [18, 19].
 Существует несколько модификаций направленных микрофонов, воспринимающих и усиливающих звуки, идущие только из одного направления, и ослабляющих все остальные звуки. В простейших из них узкая диаграмма направленности формируется за счет использования длинной трубки. В более сложных конструкциях могут использоваться несколько трубок разной длинны. Высокие параметры имеют также узко направленные микрофоны, в которых диаграмма направленности создается параболическим концентратором звука[7].
 Наиболее распространены направленные микрофоны трубчатого типа. В качестве примера можно привести ЛСТ-НМ-101 [15]. Это направленный микрофон, позволяющий прослушивать через головные телефоны и записывать на магнитофон разговор на расстояниях до 60 м. Из западных систем подобного типа широко представлены трубчатые микрофоны, закамуфлированные под зонт "в английском стиле". В него встроен усилитель и имеется выход на наушники. Реальная дальность действия не более 30 м. Теоретически, возможно создание микрофона с усилением более 20 дБ при угле менее 30 [20]. Характеристики имеющихся систем не превосходят, соответственно, 10 дБ и 90.
 Направленный микрофон органного типа представляет собой пучок из нескольких десятков тонких трубок с длинами от нескольких сантиметров до метра и более. Звуковые волны, приходящие к приемнику по осевому направлению, проходят в трубки и поступают в предкапсульный объем в одинаковой фазе, и их амплитуды складываются арифметически, а звуковые волны, приходящие под углом к оси, оказываются сдвинутыми по фазе, так как трубки имеют разную длину [20]. На сегодняшний день подобные устройства на рынке не представлены, за исключением нескольких неудачных изделий.
 В качестве примера направленного микрофона с параболическим отражателем можно привести LEA 6600 (он же "Большое ухо", он же SIPE A-2) [6]. Дальность действия на открытом месте до 1 км. Микрофон размещен в фокусе отражателя, его усиление в осевом направлении на частоте 1 кГц порядка 25 дБ. Имеется блок усиления с АРУ и выходом на наушники и магнитофон.
 Как показала практика, в реальных городских условиях невозможно проводить съем информации с расстояний, превышающих 100 м. Сотни метров могут быть достигнуты в исключительных случаях типа: заповедник, раннее утро, туман, над озером.
**2.1.3 Полуактивная система акустической разведки**

Самым оригинальным, простейшим и малозаметным до сих пор считается полуактивный радиомикрофон, работающий на частоте 330 МГц, разработанный еще в середине 40-х годов [18, 19]. Он интересен тем, что в нем нет ни источника питания, ни передатчика, ни собственно микрофона. Основой его является цилиндрический объемный резонатор, на дно которого налит небольшой слой масла. В верхней части цилиндра имеется отверстие, через которое внутренний объем резонатора сообщается с воздухом помещения, в котором ведутся переговоры. Верхняя часть сделана из пластмассы и является радиопрозрачной для радиоволн, но препятствием для акустических колебаний. В указанное отверстие вставлена металлическая втулка, снабженная четвертьволновым вибратором, настроенным на частоту 330 МГц. Размеры резонатора и уровень жидкости в нем подобраны таким образом, чтобы вся система резонировала на внешнее излучение на частоте 330 МГц. При этом собственный четвертьволновый вибратор внутри резонатора создает внешнее поле переизлучения. При ведении разговоров вблизи резонатора на поверхности масла появляются микроколебания, вызывающие изменение добротности и резонансной частоты резонатора. Этих изменений достаточно, чтобы влиять на поле переизлучения, создаваемого внутренним вибратором, которое становится модулированным по амплитуде и фазе акустическими колебаниями. Работать такой радиомикрофон может только тогда, когда он облучается мощным источником на частоте резонатора, т. е. 330 МГц. Главным достоинством такого радиомикрофона является невозможность обнаружения его при отсутствии внешнего облучения известными средствами поиска радиозакладок.
 Использование подобных систем - достаточно вредное для здоровья дело, как для тех, кого подслушивают, так и для тех, кто подслушивает.

В заключение приведем пример современной системы SIPE MM1 [7]. Пассивная радиозакладка выполнена в виде стержня длиной около 30 см и диаметром 2, 5 см. Дальность действия - 100 м. Поставляется в комплекте, состоящем из закладки, источника облучения с питанием от электросети и приемного устройства.

**2.2 Виброканал**

При воздействии акустического сигнала (речи) на поверхность твердых тел в них возникают вибрации, регистрируя которые можно прослушать интересующие разговоры. В качестве датчика используется вибродатчик, преобразующий вибросигналы в электрические.

**2.2.1Стетоскоп**

 Что это такое, можно показать на примере изделия фирмы DTI [21]. Оно состоит из вибродатчика с нанесенной на него мастикой для прикрепления к стене, блока усиления с регулятором громкости и головных телефонов. Размер датчика - 2, 2x0, 8 см, диапазон принимаемых частот - 300...3000 Гц, вес - 126 г, коэффициент усиления - 20000. С помощью подобных средств можно прослушивать через стены толщиной до 1 м. Кроме свойств вибродатчика, на качество шума влияют толщина и материал изготовления стен, уровень шумов и вибраций в обоих помещениях, правильное место выбора расположения датчика и т.д.
Однако, так как не всегда возможно постоянно находиться в соседнем помещении, вибродатчик оснащается проводным, радио- и другими каналами передачи информации, которые аналогичны тем, которые используются с микрофонами. Преимущество вибродатчиков проявляется в том, что они могут устанавливаться не в самом, зачастую тщательно охраняемом помещении, а в соседних, на которые службы безопасности обращают гораздо меньше внимания. В качестве примера приведем два устройства фирмы SIPE [7].
 Радиозакладка SIPE RS состоит из соединительного кабеля и радиопередатчика. Микрофон-стетоскоп диаметром 20 мм и высотой 34 мм обеспечивает съем информации через железобетонные конструкции толщиной до 50 см, двери и оконные рамы с двойными стеклами. На железобетон устанавливается с помощью магнита. Мощность передатчика - 20 мВт, дальность действия - 250 м. Размер передатчика 44x32x14 мм, масса 41 г, время непрерывной работы от встроенного элемента питания (ЭДС 2, 6 В) - 90 часов.
 Инфракрасная система подслушивания SIPE OPTO 2000. Состоит из миниатюрной закладки (ИК-передатчика) с линейными размерами примерно 20х30 мм со встроенным микрофоном-стетоскопом и чувствительного ИК-приемника, в состав которого входит зеркальный объектив с фокусным расстоянием 500 мм, телескопический визир и усилитель. Радиус действия передатчика - 500 м. Его излучение характеризуется широкой диаграммой направленности, что позволяет вести прием сигналов с любого удобного места.
**2.2.2 Лазерные микрофоны**

Наиболее перспективным направлением является использование лазерных микрофонов, первые образцы которых были приняты на вооружение американскими спецслужбами еще в 60-е годы. В качестве примера рассмотрим лазерное устройство HPO150 фирмы "Хъюлет Паккард" [14], обеспечивающее эффективное обнаружение, подслушивание и регистрацию разговоров, ведущихся в помещениях. Дальность действия устройства - 1000 м. Оно сконструировано на гелий-неоновом или полупроводниковом лазере с длиной волны 0, 63 мкм (что, кстати, является большим недостатком, так как пятно видно глазом, более современные системы работают в ближнем ИК-диапазоне). Прослушивание и перехват разговоров ведутся, благодаря получению отраженного сигнала от обычного оконного стекла, представляющего собой своеобразную мембрану, которая колеблется со звуковой частотой, создавая фонограмму происходящего разговора.
Приемник и передатчик выполнены раздельно. Кассетное устройство магнитной записи и специальный блок компенсации помех, а также треноги поставляются в комплекте устройства. Вся аппаратура размещена в небольшом чемодане. Электропитание - от батареи.
 Для того чтобы работать с подобной системой, требуется большой опыт. В частности, необходимо правильно выбрать точку съема, грамотно расположить аппаратуру на местности, провести тщательную юстировку. Для обработки перехваченных сообщений требуется в большинстве случаев использовать профессиональную аппаратуру обработки речевых сигналов на базе компьютера.

Была создана система с дальностью съема в 1875 м [22], однако ее можно перевозить только в грузовике. Существует опытная система ЛСТ-ЛА2, с дальностью съема порядка 60 м [25], при достаточно скромной стоимости.

**2. 3 Гидроакустические датчики**

Акустические колебания, возбуждая вибрации в трубах водоснабжения и отопления, вызывают гидроакустические сигналы в находящейся в них жидкости. Теоретически, можно перехватить обсуждаемую информацию в пределах здания с помощью гидроакустического датчика, и по имеющимся данным, такие системы испытывались. Однако очевидно, что датчик будет улавливать разговоры во всех помещениях, а, кроме того, слишком высокий уровень шумов, особенно в водопроводе. В результате остается только один путь: установить в батарее отопления передатчик в гидроакустическом диапазоне. Однако в это случае необходимо проникновение на объект (скажем, под видом сантехника, а для достоверности необходимо предварительно отключить воду в здании), что делает систему менее привлекательной.

**2. 4 Электроакустические преобразования**

При разговоре акустические волны воздействуют на конструктивные элементы электронных приборов. Они, в свою очередь, влияют на электромагнитное поле излучающих элементов или создают микроскопические токи в проводниках. Все эти токи и поля оказываются промодулированы речью и при соответствующей обработке можно извлечь полезную информацию.
Проиллюстрировать сказанное можно на примере телефона со звонком электромеханического типа. Акустические волны воздействуют на маятник звонка, соединенного с якорем электромагнитного реле. Под воздействием речевых сигналов якорь совершает микроколебания, что, в свою очередь, вызывает колебание якорных пластин в электромагнитном поле катушек, следствием чего является появление микротоков, модулированных речью.
Подобные преобразования происходят в большинстве электронных устройств (электрочасах, телевизорах, радиоприемниках и т.д.). Дальности перехвата подобных сигналов, как правило, невелики, но иногда превышают 100 м. Для усиления эффекта иногда применяется так называемое высокочастотное навязывание. В этом случае электронный прибор облучается извне мощным высокочастотным сигналом, и осуществляется прием промодулированного речью отраженного излучения. Надо сказать, что все это прерогатива спецслужб, любителям подобные действия пока не по плечу.

**3 Перехват телефонного разговора**

По заявлению Ф. Джонса, специалиста по техническим каналам связи в Нью-Йорке, в американской практике для сбора коммерческой информации конкурентов телефон используется в семнадцати случаях из ста [23].

**3.1 Подключение к линии**

Для перехвата телефонных разговоров могут быть использованы те же средства, что и для прослушивания обычных разговоров, но аппаратура должна устанавливаться у обоих абонентов. Гораздо более просто осуществить перехват путем подключения к линии. Это можно сделать как с помощью прямого физического контакта с линией, так и с помощью индуктивного датчика, т. е. не требующего врезаться в линию. На практике используются оба способа, в зависимости от типа применяемой аппаратуры.

**3.1.1 Стационарное прослушивание**

Наиболее удобно организовывать стационарное прослушивание телефонных разговоров, что достаточно просто сделать на телефонной станции (коммутаторе). В качестве примера опишу операцию по подслушиванию телефонных разговоров, проводимую американской резидентурой совместно с полицейским управлением Монтевидео [12]. Необходимые подключения к телефонным линиям на подстанциях производятся инженерами телефонной компании по просьбе полицейского управления. Шестидесятижильный кабель протянут от центрального телефонного узла в деловой части города в полицейское управление, где на верхнем этаже размещается пункт прослушивания. Там находятся исполнительные механизмы и аппаратура записи. Обслуживают пост два техника, которые передают записи в аналитический пункт.
 Если верить "Совместному решению по эксплуатационно-техническим требованиям к средствам и сетям электросвязи для обеспечения оперативно-розыскных мероприятий", опубликованному в [24], то в состав сетей электросвязи вводятся аппаратные и программные средства, позволяющие проводить контроль из удаленного пункта управления; должна быть предусмотрена возможность по командам из пункта управления изменения на определенный период категории и состава услуг, предоставляемых отдельным абонентам; должна быть предусмотрена возможность по команде из пункта управления конспиративного подключения выделенных службе безопасности каналов и линий к любым абонентским линиям (каналам), в том числе находящимся в состоянии установленного соединения.

**3.1.2 Трубка**

Чаще всего используется прослушивание разговоров с помощью существующего параллельного телефона. Есть некоторые типы аппаратов, на которых не надо даже физически поднимать трубку, так как благодаря некоторым особенностям разговор достаточно хорошо слышно (РН-299).
Если параллельного телефона нет, то достаточно просто его установить.
Для разовых операций можно использовать простейшую трубку, подключив ее к линии через копеечный резистор. Еще более просто использовать индуктивный датчик и головные телефоны. В этом случае достаточно просто приложить его к нужной линии.

**3.1.3 Диктофон**

Очень часто для записи телефонных разговоров используются диктофоны, скрытно подключенные к линии. Для подключения используются трансформаторы. Если диктофон имеет акустомат, то это идеальное устройство для записи.

Часто для записи телефонного разговора используют встроенный в аппарат магнитофон, без ведома хозяина. Однако это возможно только в случае внедрения агента.
В большинстве случаев подключение производится до распредкоробок, либо в самих распредкоробках.
Спецслужбы имеют на вооружении аппаратуру, позволяющую прослушивать переговоры, ведущиеся по подземным линиям связи. Рассмотрим принцип ее действия на примере американской системы "Крот" [25]. С помощью специального индуктивного датчика, охватывающего кабель, снимается передаваемая по нему информация. Для установки датчика на кабель используются колодцы, через которые проходит кабель. Датчик в колодце укрепляется на кабеле и для затруднения обнаружения проталкивается в трубу, подводящую кабель к колодцу. С помощью закрепленного на кабеле датчика высокочастотный сигнал, несущий информацию о ведущихся по кабелю переговорах, записывается на магнитный диск специального магнитофона. После заполнения диск заменяется новым. Запись с диска передается на установленные в помещениях спецслужб в зданиях посольств приборы демодуляции и прослушивания. В целях упрощения задачи поиска устройства "Крот" для замены диска оно снабжено сигнальной радиостанцией. Агент, проезжая или проходя в районе установки прибора-шпиона, запрашивает его с помощью своего портативного радиопередатчика, все ли в норме. Если никто не трогал, то оно передает соответствующий сигнал. В этом случае при благоприятных условиях агент заменяет диск в магнитофоне и работа устройства продолжается. Аппарат может записывать информацию, передаваемую одновременно по 60 телефонным каналам. Продолжительность непрерывной записи разговора на магнитофон составляет 115 ч.

Для различных типов подземных кабелей разработаны разные подслушивающие устройства: для симметричных высокочастотных кабелей - устройства с индуктивными датчиками, для коаксиальных и низкочастотных кабелей - с системами непосредственного подключения и отвода малой части энергии для целей перехвата. Для кабелей, внутри которых поддерживалось повышенное давление воздуха, применяются устройства, исключающие его снижение, в результате чего предотвращается срабатывание специальной сигнализации. Некоторые приборы снабжаются радиостанциями для прямой передачи подслушанных разговоров в центр их обработки, но это уже тема следующего раздела.

**3.1.4 Телефонный радиотранслятор**

Телефонные закладки могут подключатся к любой точке телефонной линии и иметь неограниченный срок службы, так как питаются от телефонной сети.
Большинство телефонных закладок представляют собой специальные радиозакладки. Они автоматически включаются при поднятии телефонной трубки и передают по радиоканалу телефонный разговор на пункт перехвата, где он может быть прослушан и записан. Так как телефонный аппарат имеет свой микрофон и закладкам не нужен источник питания, их размеры могут быть миниатюрными.
Наиболее распространены изделия типа ЛСТ-5. При габаритах 22x14x13 мм он излучает на фиксированной частоте в диапазоне 60...170 МГц на расстояние до 400 м, а при подключении антенны, до 1000 м. Частоту можно изменить самостоятельно в пределах 10 МГц [15].
Более совершенные, хотя и со значительно меньшей дальностью закладки выпускаются в виде конденсаторов, которые устанавливаются в самом телефонном аппарате или в розетке (ЛСТ-5К). Выпускаются также комбинированные системы обеспечивающие прослушивание и телефонов и помещений (ЛСТ-5-1). Интересное изделие предлагает фирма SIPE. Изделие TK CRISTAL сделано в виде микрофона телефонного аппарата и может быть установлена в него за несколько секунд. Частота передатчика стабилизирована кварцем. Дальность действия 150 м.

**3.1.5 Побочные электромагнитные сигналы и наводки**

Любое электронное изделие при работе излучает так называемые побочные электромагнитные излучения и наводки. Очень распространены телефоны с кнопочным номеронабирателем типа ТА-Т, ТА-12 и т.д. При наборе номера и ведении переговоров благодаря техническим особенностям блока питания вся информация ретранслируется на десятках частот в СВ, КВ и УКВ диапазонах на расстояние до 200 м. В случае применении подобного телефона радиозакладки не нужны.

Обычно перехват осуществляется более сложно. С помощью малогабаритного индуктивного датчика можно улавливать побочные электромагнитные колебания автотрансформатора практически любого телефонного аппарата на расстоянии до полуметра. При этом также регистрируются набираемые номера и все разговоры.
 **3.2 Перехват разговоров по радиотелефону**

 Радиотелефон - это комплект из двух радиостанций, одна из которых является базовой, устанавливается стационарно и подключается к телефонной сети, вторая - подвижная. От обычной радиостанции отличается тем что пользователь радиотелефона выходит непосредственно в городскую телефонную сеть [26]. Следовательно, осуществлять прослушивание телефонных разговоров можно теми же способами, которые описаны в разделе 3. 2.
При наличии сотовой связи в регионе можно стать ее абонентом, при этом качество связи (помехозащищенность) будет значительно лучше. Но при этом можно применять те же способы прослушивания.
Дальность действия радиотелефона зависит от диапазона частот, в котором он работает, от выходной мощности и применяемой антенны. В диапазоне УКВ на дальность радиосвязи влияют также рельеф местности и наличие различных построек. Дальность действия "беспроводных" телефонов редко превышает 300 м. Остальные радиотелефоны работают на дальностях от 1 до 100 км.
С точки зрения съема информации радиотелефоны, в том числе сотовые системы, и радиостанции объединяет то, что при работе они используют радиоволны. Нет необходимости устанавливать радиомикрофоны телефонные закладки, использовать лазерные микрофоны или стетоскопы, достаточно приобрести качественный приемник, установить хорошую антенну и спокойно прослушивать разговоры. При этом дальность радиоперехвата будет не менее дальности работы радиотелефона, а при использовании хорошей аппаратуры - в несколько раз больше. Кроме того, по излучаемым сигналам можно установить местонахождение автомобиля, оборудованного радиотелефоном.
 Наиболее совершенным среди портативных универсальных разведывательных приемников является Miniport фирмы "Роде и шварц" с диапазоном частот 20...1000 МГц. С помощью его можно без труда осуществлять перехват всех без исключения радиостанций и радиотелефонов. Описываемый приемник имеет малые габариты, универсальное питание (от аккумуляторной батареи и от сети) и может успешно применятся в стационарных полевых условиях. Управление приемником осуществляется цифровым способом через встроенный процессор. Визуальное считывание значения частоты производится с цифрового дисплея с шагом 1 кГц. Запоминающее устройство микропроцессора может запоминать до 30 значений частоты, может осуществлять сканирование с переменным шагом. Возможности приемника могут быть расширены за счет совмещения с малогабаритным анализатором спектра, специально разработанного для него - типа EPZ100. Для удобства применения комплекса аппаратуры в полевых условиях изготавливаются специальные вспомогательные кейсы, где отдельно размещается аккумулятор, приемник с анализатором спектра и набор антенн[26, 28].
 Для определения точного местоположения источника нужно иметь несколько, по крайней мере два пеленгатора, чтобы сделать "засечку" в месте пересечения двух пеленгов одного источника с разных мест. В последнее время появились более совершенные пеленгаторы доплеровского типа, у которых нет механически вращающихся антенн, а есть одна антенная мачта, на которой размещено более десяти идентичных диполей. За счет специальной обработки сигнала производится мгновенная пеленгация излучателя.
При совмещении подобной антенны с описанным выше приемником возможно за 0,1 с обнаружить радиосигнал, измерить его параметры и взять пеленг. С учетом необходимости передачи данных на другой пост пеленгации с целью однозначного определения местоположения источника излучения требуется около 1...2 с. для точного знания места [19]. Таким образом, не успев сказать несколько слов по радиотелефону, абонент точно указывает местоположение своего автомобиля.
В целом ряде случаев используются специальные радиомаяки, которые скрытно устанавливаются в автомобилях, а в некоторых случаях вшиваются в одежду, монтируются в дипломат и т.д. для обеспечения контроля за перемещением объекта наблюдения по городу.
 Специалисты утверждают, что перехват может осуществляться и при передаче обычных междугородных телефонных переговоров (а также телеграфных, факс и т.д.) через спутник связи, либо по радиорелейным линиям.

**4 Несанкционированное получение документа на небумажном носителе**

В настоящее время все большее количество информации оказывается сосредоточенным на небумажных носителях. К ним, в первую очередь, относятся жесткие диски и дискеты персональных компьютеров, перфоленты и перфокарты кое-где сохранившихся у нас ЭВМ 60-70-х годов, микрофильмы и кинопленки, аудио- и видеокассеты, лазерные диски. Особое внимание следует обратить на персональные компьютеры (ПК), по следующим объективным причинам:
• высокие темпы роста парка ПК, находящихся в эксплуатации;
• широкое применение ПК в самых различных сферах человеческой деятельности;
• высокая степень концентрации информации в ПК;
• усложнение вычислительного процесса в ПК [33].
Однако рост числа компьютеров и развитие информационных сетей породило целый ряд проблем. Появилась новая отрасль связанная с извлечением информации из систем обработки данных (СОД).
В связи с тем, что гигантские массивы информации хранятся на небумажных носителях, доступ к ним имеет наибольший интерес. Потенциальным объектом может быть любая информация находящаяся на носителях.

**5 Несанкционированный перехват небумажного документа в процессе его обработки**

При обработке небумажного документа возникают некоторые дополнительные возможности для несанкционированного съема информации. Самое важное, что при этом в большинстве случаев не требуется проникновение на объект.

**5.1 Побочные электромагнитные сигналы и наводки**

При работе электронной техники образуются побочные электромагнитные излучения и наводки на провода, кабели и прочие токопроводящие коммуникации (трубы, арматуру и т.д.). Наиболее вероятен перехват сведений при приеме излучений от дисплеев, накопителей на магнитных дисках, принтеров и соединительных кабелей.
Проще всего снять информацию с дисплея. Изображение на экране формируется, в основном, так же, как и в телевизионном приемнике. Видеосигнал, необходимый для получения изображения, модулирует ток электронного луча. Таким образом, он является цифровым сигналом, логическая единица которого создает световую точку, а логический ноль препятствует ее появлению. Кроме того, в цепях дисплея присутствуют тактовые синхроимпульсы.
 Источниками излучения видеосигнала могут быть элементы обработки сигнала изображения и электронный луч кинескопа. В отличие от других сигналов, существующих в ПК, видеосигнал усиливается до нескольких десятков киловольт для подачи на электронно-лучевую трубку. Следовательно, видеоусилитель является наиболее мощным (и опасным) источником широкополосного излучения. Источником же узкополосного излучения является система синхронизации.
Излучение дисплеев, содержащих гармоники видеосигналов, охватывает диапазон метровых и дециметровых волн. На некоторых частотах (например, 125 и 210 МГц - чуть выше пятого и десятый телевизионные каналы соответственно) имеются резонансы, которые являются причиной усиления излучения относительно соседних частот.
Информация, отображенная на дисплее, может быть восстановлена с помощью бытового телевизора. Настроившись на один из "лепестков" энергетического спектра излучения, получаем копию изображения дисплея, состоящую из белых букв на черном (сером) фоне.
Но излучение дисплея, принимаемое телевизором, не содержит информации о синхросигнале, поэтому изображение на экране ТВ-приемника перемещается в горизонтальном и вертикальном направлениях. Качество приема может быть улучшено с помощью внешнего генератора синхросигналов, подаваемых на приемник. С такой приставкой к обычному телевизору можно восстановить информацию с дисплея любого типа (в том числе, монитора системы сигнализации и т.д.) при условии достаточно высокого уровня его излучения. Сигналы на выходе генератора должны иметь частоты 15...20 кГц для синхронизации строк и 4-...80 кГц для синхронизации кадров [38].
Для неспециалиста не составит труда снять информацию таким способом на расстоянии до 10 м (за стеной). Используя специальную антенну и усилитель, профессионал успешно выполнит задание при расстоянии до 150 м.
Вторым по важности каналом утечки информации являются квазистационарные информационные магнитные и электрические поля, излучаемые головками накопителей на гибких и жестких магнитных дисках, кабелями, элементами схем и т.д. Эти поля быстро убывают с расстоянием, но вызывают наводки на любые проводящие цепи (телефонные провода, металлические трубы и т.д.). При этом максимумы излучения находятся в диапазоне от десятков килогерц до десятков мегагерц. Наиболее просто восстанавливаются излучения, возникающие при функционировании накопителей на магнитных дисках [39]. В качестве примера можно сослаться на устройство, с помощью которого можно выявлять номера банковских счетов и коды доступа к ним во время введения кредитной карточки (магнитной) в автомат, выдающий наличные. Кроме того, не составляет большого труда восстановить информацию, наводимую по цепям питания. При этом установленные на многих машинах защитные сетевые фильтры не являются надежной преградой.

**5.2 Аппаратные закладки**

Перехват побочных электромагнитных излучений и наводок довольно хлопотное дело, а восстановление сигналов - удел профессионалов. Подобные операции стоят дорого, а эффект дают не всегда (за исключением перехвата излучения дисплеев). В связи с этим ясно стремление установить специальные устройства в вычислительной технике, которые, питаясь от ее источников напряжения, месяцами передавали бы информацию на какой-то фиксированной частоте на значительные расстояния (до 2 км). Наиболее перспективным в этом плане является внедрение подобных устройств в клавиатуру, накопители на магнитных дисках и т.д.
**5.3 Программные закладки**

Перспективным направлением является внедрение программных закладок. Их задачей может быть получение информации о паролях, кодовых комбинациях, обрабатываемых данных и передача собранных сведений заданному адресу по сети, электронной почте и т.д. Способы установки те же, что и для компьютерных вирусов, да и сами закладки, по существу, являются вирусами. В настоящее время известны следующие основные механизмы проникновения вирусов [40].
 Непосредственное подключение - передача вирусов через средства обмена, используемые в атакуемой системе. Собственно внедрение производится через наименее защищенные узлы системы либо поставкой "зараженного" программного обеспечения.
 Косвенное подключение - это приемы проникновения в систему через подсистемы, непосредственно не служащие ее основному предназначению (электропитание, стабилизация и т.д.), не обязательно построенные на электрических связях с процессорами. Один из приемов - внедрение вирусов путем подачи рассчитанных электромагнитных импульсов в схему питания. Над этим вопросом особенно усиленно работают японцы и американцы.

**6 Перехват документа на небумажном носителе при его передаче**

В настоящее время гигантское количество информации передается по различным каналам связи, причем, как правило, используется телефонная сеть. Получают все большее развитие такие сервисные службы, как электронная почта, телекс, факс, телетекст, видеотекст, передача биржевой информации, банковские операции и т.д. Главным недостатком использования телефонной связи для передачи данных является ее доступность для любого лица, располагающего соответствующей аппаратурой.
 Способы, используемые для перехвата передаваемых сообщений, в основном, те же, что и для подслушивания телефонных разговоров. Рассмотрим это на примере факсимильной связи (факса), поскольку многие бизнесмены считают, что это самый безопасный вид связи. На самом деле передаваемые тексты может перехватывать любой человек с помощью устройства, которое стоит несколько сотен долларов. А японская компания "Ниппон телефон энд телеграф" сообщила о том, что располагает доказательствами подключения к ее факсам не только в Японии, но и во всем мире.
Для передачи информации также распространенным является отправка ее по ошибочным адресам. Дело в том, что человек достаточно часто ошибается в наборе номера, и если в случае обычного телефонного разговора он сразу понимает, что говорит не с тем человеком, то при отправке сообщения по компьютерной сети или факсу этого не происходит. Кроме того, отправляя информацию по правильному адресу, часто не проверяют, кто конкретно ее принял, а этим человеком может быть злоумышленник.

**Заключение**

В данной работе отражены основные методы нештатного доступа к информации, технические средства и параметры по которым производится считывание информации. Так же приведены примеры обеспечения защиты информации. Цель курсовой дать реальное представление о возможностях нештатного съема информации.

**Литература**

1. Введение в философию. М., Издательство политической литературы. 1989. С. 312.
2. Даллес А. Искусство разведки. М., Международные отношения. 1992. С. 288.
3. Розенберг В. Промысловая тайна. СПб., Типография редакции Министерства финансов. 1910.
4. Мальцева О. Защищайтесь, господа! Деловые люди. 1992, июнь. С. 90.
5. Вольтон Т. КГБ во Франции: Пер. с фр. Издательская группа "Прогресс". 1993. С. 336.
6. Каташинский А. Реорганизация разведывательных служб США. Зарубежное военное обозрение. 1993, N 3. С. 9-12.
7. Предпринимательство и безопасность. М., Универсум. 1991. Т. 1-3.
8. Бизнес и безопасность. М., КМЦ "Центурион". 1992.
9. Никакого снисхождения. Красная Звезда. 1993. 21 мая.
10. Гасанов Р. М. Шпионаж особого рода. М., Мысль. 1989. С. 254.
11. Ярочкин В. Проблемы информационной безопасности. Частный сыск и охрана? 1993. N 9. С. 55-56.
12. Эйджи Ф. За кулисами ЦРУ: Пер. с англ. М., Вонениздат. 1979. С. 464.
13. Гасанов Р. М. Промышленный шпионаж на службе монополий. М., Политиздат. 1989. С. 267.
14. Вартанесян В. И. Радиоэлектронная разведка. М., Военное издательство. 1991. С. 254.
15. Лаборатория спецтехники. Каталог. 1994. С. 5.
16. Spy HeadQuarters. Produkt Catalog. P. 35.
17. Donald F. B. Robot Spies of KGB. -Signal. 1989. Vol. 44. N 4. P. 79-83.
18. A Espionagem Electronica/ Antenne. 1976. Outburo. Vol. 76. N 4. P. 323-328.
19. Технические средства разведки/ Под ред. В. И. Мухина. М., РВСН. 1992. С. 334.
20. Сапожков М. А. Электроакустика. М., Связь. 1978. С. 272.
21. Sound Detector. Instruction Manual. DTI. 1990. P. 5.
22. Балкарей И. Е. Дистанционная регистрация малых колебаний через атмосферу СО 2-лазерным гетеродинным устройством. Квантовая электроника. 1989. С. 1494-1498.
23. Наумов А. Алло! Вас подслушивают. Деловые люди. 1992, июль-август. С. 92-94.
24. "Большое ухо" КГБ в каждом российском доме. Час Пик. N 8, 3. 3. 93. C. 2.
25. Брусницын Н. А. Открытость и шпионаж. М., Военное издательство. 1991. С. 56.
26. Частный сыск и охрана. 19993. N 9. C. 62-63.
27. Miniport Receiver EB 100 (20 to 1000 MHz) // Rohde Schwarz. Munich. FRD. 1991. P. 8.
28. Accessories for Miniport Receiver EB 100 // Rohnde Schwarz. Munich. FRD. 1990. P. 1, 2.
29. Панарин И. Космическая явка шпиона. Советская РОссия, N 69. (10220), 25 марта 1990.
30. Инструмент тотального шпионажа. Красная Звезда, 29. 12. 89.
31. Defence. 1986, may. P. 208-209.
32. Wohin Jhre Kunden auch reisen...Agfamatic 901E // Foto contract. BRD. N 3. P. 1, 83.
33. Спесивцев А. В и др. Защита информации в персональных ЭВМ. М., Радио и связь, МП "Веста". 1992. С. 192.
34. Информатика в жизни США. UCIA. 1988. P. 54.
35. Герасименко В. А., Размахнин М. К. Организация работ по защите информации в системах электронной обработки данных. Зарубежная электроника. 1989, N 12.
36. Герасименко В. А. Проблемы защиты данных в системах их обработки. Зарубежная электроника. 1989, N 12. С. 5-21.
37. Компьютер: друг или враг? Деловые люди. N 12. C. 89.
38. Маркин А. В. Безопасность излучений и наводок от средств электронно-вычислительной техники. Зарубежная радиоэлектроника. 1989. N 12. С. 101-109.
39. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. КомпьютерПресс. 1993. N 10. C. 33.
40. Семенов Н. С. Компьютерные вирусы как средство электронной борьбы. Судостроение за рубежом. 1990. N 12. C. 48-61.
41. http://rapidlinks.ru/
42. http://macmil.stsland.ru/spionas.htm