Министерство образования и науки РФ

Российский государственный гуманитарный университет

Факультет защиты информации

Кафедра
инженерно-технической
защиты информации

Богданов Андрей Юрьевич

Разработка комплексной системы требований по защите объекта информатизации

Курсовая работа

студента 5 курса дневного отделения

Студент

Научный руководитель
проф., к.т.н. Д.Б. Халяпин

Отметка _____

Москва 2005

Оглавление

Список иллюстраций

Список таблиц

Введение

В работе рассматривается формирование комплексной системы требований по защите объекта информатизации на примере конкретного помещения (помещение №4.04 подразделения информационных технологий ЗАО "СПиС" на объекте, расположенном в Москве). Разработка таких требований происходит с учетом технических средств защиты информации и технических средств охраны. При этом учитывается ряд нормативных документов, изданных Гостехкомиссией России и МВД РФ (государственные стандарты, руководящие документы, временные методики).

Таким образом, целью данной работы является разработка предложений по созданию комплексной системы требований по защите объекта информатизации с учетом комплекса требований по инженерно-технической защите информации и охране. При этом используются следующие нормативные документы:

- РД 78.36.003-2002 "Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств" МВД РФ,
- ГОСТ Р51558-2000 "Системы охранные телевизионные. Общие технические требования и методы испытаний",
- "Временная методика оценки защищенности речевой конфиденциальной информации от утечки по акустическому и виброакустическому каналам" Гостехкомиссии России, 2001 год.

Для достижения указанной цели необходимо решить следующие задачи:

- определение подгруппы защищаемого объекта, в котором содержится конфиденциальная информация,
- определение соответствия инженерной укрепленности помещения требованиям по РД 78.36.003-2002 и формирование предложений по улучшению характеристик инженерных конструкций в соответствии с выбранной подгруппой объектов,

- формирование требований к системе охранной сигнализации по РД 78.36.003-2002 для данной подгруппы объектов и выбор конкретных моделей охранных извещателей,

- формулировка требований к системе видеонаблюдения для выбранной подгруппы объектов по ГОСТ Р51558-2000 и РД 78.36.003-2002 и предложение по выбору конкретных моделей средств видеонаблюдения,

- формулировка требований к защите конфиденциальной речевой информации от утечки по воздушному акустическому, виброакустическому, акустопреобразовательному и другим каналам (см. набор каналов утечки в разделе 1) и формирование предложений по защите такой информации с учетом конкретных моделей соответствующих технических средств защиты информации (при решении данной задачи необходимо основываться на на требованиях, сформулированных во "Временной методике оценки защищенности речевой конфиденциальной информации от утечки по акустическому и виброакустическому каналам" Гостехкомиссии России),

- формулировка требований к защите конфиденциальной информации от утечки по оптическому каналу,

- формулировка требований к защите конфиденциальной информации, передаваемой по телефонным линиям, расположенным в защищаемом помещении, и выбор соответствующих моделей технических средств защиты информации,

- формулировка требований к защите конфиденциальной информации, обрабатываемой на ПЭВМ, расположеной в данном помещении, по ПЭМИН и выбор соответствующих технических средств защиты информации.

Указанные цели и задачи определяют структуру работы. В разделе 1 описывается объект защиты, выбираются направления защиты информа-

ции на объекте в соответствии с назначением объекта. В разделе 2 выдвигаются требования к инженерной укрепленности объекта. В разделе 3 описываются требования к системе охранной сигнализации и техническим средствам видеонаблюдения. В разделе 4 формулируются требования к комплексной защите акустической информации на объекте, а также к защите информации от утечки по оптическому каналу. В разделе 5 описываются требования к защите конфиденциальной информации в телефонных линиях и ПЭВМ, расположенных на объекте.

1 Описание объекта защиты и выбор направлений защиты

В качестве объекта защиты было выбрано помещение №4.04 подразделения информационных технологий ЗАО "СПиС" в г. Москва. В этом разделе дается детальное описание данного помещения, определяется его класс в соответствии с РД 78.36.003-2002 ГУ Вневедомственной охраны Министерства внутренних дел РФ. Помимо этого, здесь происходит выделение релевантных направлений инженерно-технической защиты информации в помещении, исходя из всего спектра технических каналов утечки информации.

Опишем защищаемое помещение, его расположение в пределах здания ЗАО "СПиС" и размещение этого здания относительно других строений и улиц.

Принимается, что помещение предназначено для проведения конфиденциальных переговоров и совещаний, работы с конфиденциальными документами, обработки конфиденциальной информации с использованием ПЭВМ, проведения конфиденциальных телефонных переговоров.

В защищаемом помещении (см. рис. 1) находится стол для проведения конфиденциальных переговоров. Считается, что источник конфиденциальной акустической информации может находиться только в области этого стола. Рядом со столом расположен сейф для хранения материальных но-

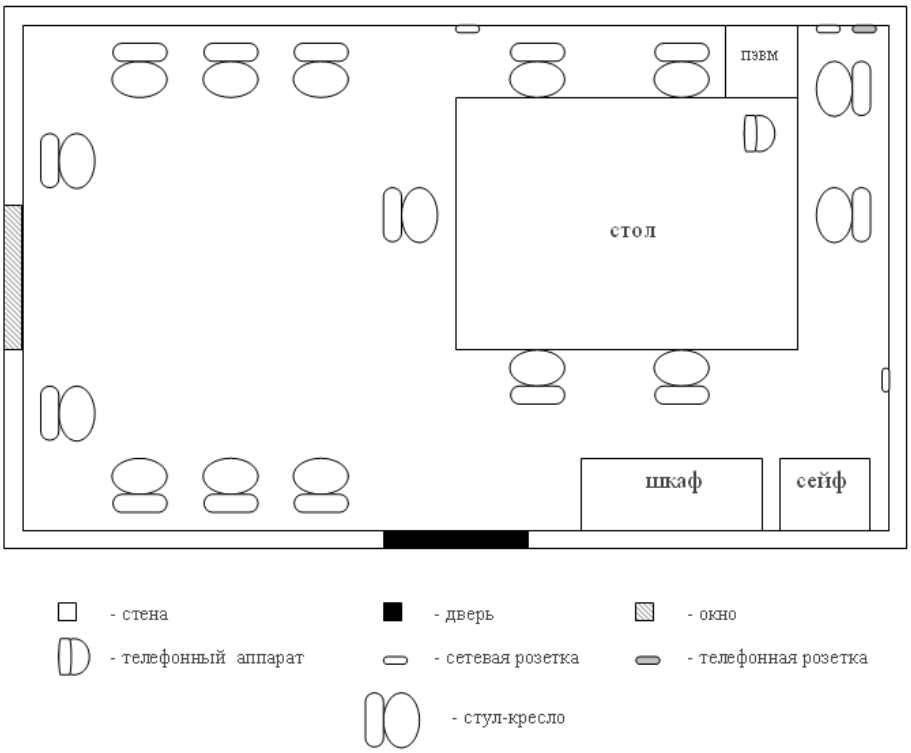

Рис. 1: План-схема защищаемого помещения № 4.04 ЗАО "СПиС".

сителей конфиденциальной информации (конфиденциальные документы, дискеты, CD- и DVD-диски). На столе находится телефонный аппарат, который используется для конфиденциальных переговоров, подключенный к телефонной линии через телефонную розетку. Рядом с телефоном установлен компьютерный стол с ПЭВМ, используемой для хранения и обработки конфиденциальной информации. ПЭВМ подключена только к электрической сети, и у нее нет выхода в локальную сеть и более крупные компьютерные сети. Имеются также 2 неиспользуемые розетки сети электропитания. В помещении располагается шкаф, не предназначенный для хранения каких-либо носителей конфиденциальной информации, и несколько стульев.

На рис. 2 представлено расположение помещения относительно других помещений, находящихся на этаже здания. Защищаемое помещение находится на 4-м этаже 7-миэтажного здания. Предприятию принадлежит все строение полностью. Дверь защищаемого помещения выходит в комнату №4.05, откуда возможен выход в коридор. Считается, что ни в каких дру-

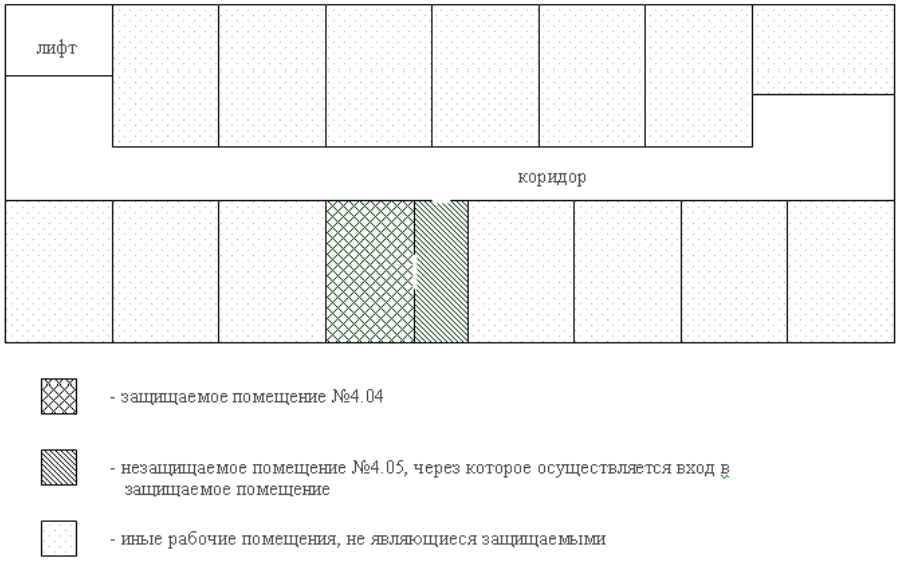

Рис. 2: План-схема расположения защищаемого помещения № 4.04 в здании ЗАО "СПиС" на 4-ом этаже.

гих помещениях данного этажа, а также в помещениях этажом выше и этажом ниже, смежных с защищаемым, работа с конфиденциальной информацией не проводится. Эти помещения не являются защищенными.

Стены и перекрытия помещения выполнены из пустотных железобетонных плит толщиной 300 мм из легких бетонов. Дверь помещения изготовлена из дерева со сплошным заполнением полотен толщиной 50 мм. Запирающее устройство в виде врезного штифтового замка с 8-ю кодовыми штифтами.

Здание расположено в некотором отдалении от проезжей части и других домов (см. рис. 3). В помещении имеется одно окно, выходящее в сторону, противоположную проезжей части. Окно не примыкает к пожарным лестницам, которые расположены на торцах здания. Балконов в здании нет. Оконные конструкции выполнены с применением обычного стекла толщиной 4 мм. Окна двойные.

Рассматриваемое помещение, в соответствии с РД 78.36.003-2002, относится к группе А объектов. Подгруппа данного объекта определяется как АII в соответствии с предположением, что на данном объекте хранится и обрабатывается конфиденциальная информация. К категории АII, по ука-

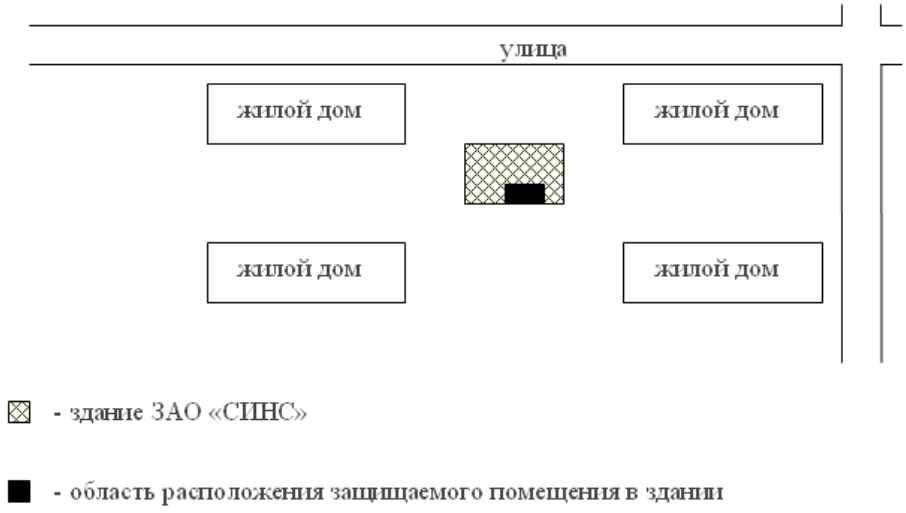

Рис. 3: План-схема расположения здания ЗАО "СПиС" и защищаемого помещения относительно других строений и улиц.

занному РД 78.36.003-2002, относятся специальные помещения особо важных объектов и объектов повышенной опасности. Это помещения, в которых размещаются материальные ценности второй категории. К ним относятся: хранилища и кладовые денежных и валютных средств, ценных бумаг; хранилища ювелирных изделий, драгоценных металлов и камней; хранилища секретной документации, изделий; специальные хранилища взрывчатых, наркотических, ядовитых, бактериологических, токсичных и психотропных веществ и препаратов; специальные фондохранилища музеев и библиотек. Из этого перечня и из предназначения помещения следует, что защищаемый объект относится к подгруппе AII.

В разделах 2 и 3 описываются требования к инженерной укрепленности, системам охранной сигнализации и системы видеонаблюдения для объекта подгруппы AII, а также даются предложения по повышению инженерной укрепленности объекта, описываются конкретные предложения по моделям элементов систем охранной сигнализации и видеонаблюдения в соответствии с РД 78.36.003-2002 и ГОСТ Р51558-2000.

Выявим технические каналы утечки информации из защищаемого помещения и опишем их реализации, возможные в данном случае.

Проведенный анализ обстановки в защищаемом помещении приводит к выделению следующих возможных каналов утечки информации:

- канал утечки акустической информации воздушной волной (акустический канал);
- канал утечки акустической информации структурной волной (виброакустический канал);
- оптический канал утечки графической и текстовой информации непосредственно с конфиденциальных документов на традиционных носителях, а также за счет их визуального представления на экране ПЭВМ;
- канал утечки акустической информации с использованием облучающих сигналов (акусто-оптический или оптико-электронный канал);
- канал утечки акустической информации за счет акустоэлектрических преобразователей (акустопреобразовательный канал);
- канал утечки акустической информации за счет применения закладных устройств (по линиям питания, управления, радиосигналом и т.д.), нелегальных звукозаписывающих устройств и за счет несанкционированной передачи акустики помещения по сотовому телефону;
- канал утечки информации за счет ПЭМИН;
- канал утечки информации за счет прослушивания телефонных переговоров.

Рассмотрим каждый из этих каналов более подробно.

Утечка акустической информации за счет воздушной волны может в защищаемом помещении происходить через стены, перекрытия (пол, потолок), окно, дверь и вентиляционную трубу. От данного канала можно защищаться пассивными, активными и комбинированными методами. Пассивные методы основаны на ослаблении акустических (речевых) сигналов

на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов. Активные методы базируются на создании маскирующих акустических и вибрационных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного акустического сигнала средством разведки.

Утечка акустической информации за счет структурной волны из защищаемого помещения может происходить через стену, перекрытия (потолок и пол) и дверь. Активные, пассивные и комбинированные методы защиты от данного канала по принципу применения совпадают со случаем утечки по воздушной волне.

Непосредственная утечка по оптическому каналу может происходить через окно. Естественная защита от такого канала - это экранирование, исключающее прямую видимость объекта со стороны злоумышленника. Возможна также утечка при несанкционированных фотографировании и видеозаписи, в том числе и при несанкционированном применении установленной в помещении охранной ТВК.

Канал утечки акустической информации с использованием облучающих сигналов в защищаемом помещении может возникать за счет облучения элементов инженерной конструкции помещения или деталей интерьера помещения неинформативным ИК- или СВЧ-сигналом и последующего приема этого сигнала, промодулированного информативным сигналом. Защита может заключаться в генерации вибрационных помех на чувствительных элементах инженерных конструкций (активная защита) и локализации предметов, вибрации которых модулируются акустическим речевым сигналом (пассивная защита).

Канал утечки акустической информации за счет акустоэлектрических преобразователей может возникнуть за счет акустопреобразовательных процессов в розетках электропитания, телефонном аппарате, телефонной розетке, извещателях охранной сигнализации, аппаратуре электроосвещения, ТВК (линии связи и управления) и элементах ПЭВМ. Пассивным методом защиты от этого канала утечки является ослабление информацион-

ных электрических сигналов в соединительных линиях и линиях питания ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов. Активная защита заключается в создании маскирующих электромагнитных помех в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

Закладные устройства можно локализовывать с помощью специальных технических средств (пассивная защита). Активная защита заключается в зашумлении каналов передачи информации от закладного устройства к злоумышленнику (радиоканал, линии сингализации, линии связи и управления ТВК, линии электропитания). Сотовые телефоны можно подавлять специальными техническими средствами (активная защита) или экранировать (пассивная защита). Диктофоны можно обнаруживать по побочному электромагнитному излучению (пассивная защита) и подавлять электромагнитным и ультразвуковым излучением (активная защита).

Канал утечки по ПЭМИН можно перекрыть путем электромагнитного экранирования отдельных элементов ПЭВМ, ПЭВМ в целом, а также всего помещения (пассивная защита). Активная защита состоит в подавлении опасных сигналов применением генераторов пространственного и линейного зашумления.

От утечки информации за счет прослушивания телефонных переговоров можно защищаться пассивными методами, заключающимися в обнаружении несанкционированных подключений к телефонным линиям связи, и активными методами, состоящими в создании прицельных радиопомех телефонным радиозакладкам с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки, подавлении (нарушении функционирования) средств несанкционированного подключения к телефонным линиям, уни-

чтожении (выводе из строя) средств несанкционированного подключения к телефонным линиям.

2 Требования к инженерной укрепленности объекта

Рассмотрим требования к инженерной укрепленности объекта подгруппы AII по РД 78.36.003-2002 и дадим предложения по повышению уровня инженерной укрепленности защищаемого объекта.

Требования к инженерной укрепленности связаны с категорией объекта. Каждой подгруппе объектов (AI, AII, БI, БII) и каждому конструктивному элементу (стены, двери, окна и т.д.) инженерно-технического комплекса объекта соответствует определенный класс требуемой защищенности. Этот класс характеризуется определенными конкретными инженерно-техническими мероприятиями относительно данного элемента. Так, для объекта подгруппы AII рассматриваются следующие конструктивные элементы инженерно-технического комплекса:

в части строительных конструкций: наружные стены охраняемого помещения на втором и выше этажах, а также стены и перекрытия внутри блока помещений одного собственника - по классу 3; внутренние стены, перегородки в пределах подгруппы - по классу 1;

в части дверных конструкций: входные двери помещения - по классу 4; внутренние двери в пределах подгруппы - по классу 1;

в части запирающих устройств: запирающие устройства входных дверей помещения - по классу 4; запирающие устройства внутренних дверей помещения - по классу 1;

в части оконных конструкций: оконные проемы 2-го и выше этажей, не примыкающие к пожарным лестницам, балконам, - по классу 2.

В РД 78.36.003-2002 даются описания элементов инженерной конструкции объекта в соответствии с требуемыми классами защищенности. Приведем относящиеся к данному случаю описания с указанием мер, которые необходимо принять для повышения класса защищенности элемента до требуемого.

Наружные стены охраняемого помещения на втором и выше этажах, а также стены и перекрытия внутри блока помещений одного собственника - по классу 3: 3-я степень защищенности соответствует высокой степени защиты объекта от проникновения. В целях разумного использования существующих строительных конструкций (пустотные железо-бетонные плиты толщиной 300мм из легких бетонов), соответствующих 2-му классу защищенности, был выбран следующий вариант строительных конструкций 3-го класса защищенности: строительные конструкции 2-го класса, усиленные стальной сеткой с толщиной прутка 8 мм и с ячейкой 100x100 мм. Таким образом, для повышения класса защищенности строительных конструкция до уровня, соответствующего объекту класса А II, предлагается укрепить стены, потолок и пол помещения указанной стальной сеткой.

Входные двери помещения - по классу 4: 4-я степень защищенности соответствует специальной степени защиты от проникновения. Здесь для повышения класса защищенности входной двери можно использовать один из следующих вариантов:

- двери, соответствующие категории и классу устойчивости С-II и выше по ГОСТ Р 51242-98;
- двери защитных кабин по ГОСТ Р 50941-96;
- защитные двери по ГОСТ Р 51072-97;
- двери для хранилищ и сейфовых комнат по ГОСТ Р 50862-96.

Т.к. используемые в помещении двери соответствуют лишь 2-му классу защищенности, то предлагается демонтировать их и установить

дверь, соответствующую одному из перечисленных вариантов. При этом можно пользоваться рекомендуемыми способами усиления дверных конструкций по РД 78.36.003-2002. Кроме этого, предлагается установить с внутренней стороны этой двери еще одну дверь - решетчатую металлическую 2-го класса защищенности, изготовленную из стальных прутьев диаметром не менее 16 мм, образующих ячейку не более 150×150 мм и свариваемых в каждом пересечении. По периметру эта дверь обрамляется стальным уголком размером не менее 35×35×4 мм. Основная дверь открывается во внешнюю сторону, а дополнительная - во внутреннюю.

Запирающие устройства входных дверей помещения - по классу 4: 4-я степень защищенности соответствует специальной степени защиты от проникновения. Этому классу соответствуют следующие врезные замки:

- класса 4 по ГОСТ 5089-97;
- сейфовые по ГОСТ Р 51053-97, количество и класс которых выбирается в зависимости от класса устойчивости двери.

Используемые в настоящее время замки соответствуют лишь 2-му классу защищенности. Поэтому предлагается их демонтировать вместе с дверной конструкцией и установить в новую дверь врезной замок по одному из указанных вариантов. Дополнительную же решетчатую дверь предлагается оборудовать сувальдным накладным замком с количеством сувальд не менее 5, который соответствует 2-му классу защищенности.

Оконные проемы 2-го и выше этажей, не примыкающие к пожарным лестницам, балконам, - по классу 2: 2-я степень защищенности соответствует средней степени защиты объекта от проникновения. Для повышения существующего класса защищенности оконных конструкций (1 класс) до 2-ого класса предлагается усилить их металлическимм решетками

произвольной конструкции, изготовленными из стальных прутьев сечением не менее 78 мм^2, образующих ячейку площадью не более 230 см^2 и свариваемых в каждом пересечении. Данную решетку предлагается разместить между первым и вторым слоями остекления. Окно при этом становится неоткрываемым.

3 Требования к охране объекта и рекомендуемые ТСО

Из всего набора технических средств охраны будем рассматривать лишь 2 типа: системы охранной сигнализации и системы телевизионного видеонаблюдения. В указанных системах будем рассматривать только те их элементы, которые располагаются в защищаемом помещении или непосредственно связаны с последними: в случае систем охранной сигнализации к таким элементам относятся охранные извещатели и шлейфы сигнализации, а в случае систем видеонаблюдения - телевизионные камеры и соединительные линии (кабели).

В соответствии с РД 78.36.003-2002 техническими средствами охранной сигнализации должно оборудоваться защищаемое помещение, а также все уязвимые места помещения (окна, двери, люки, вентиляционные шахты, коробы и т.д.), через которые возможно несанкционированное проникновение. Объекты подгруппы AII оборудуются многорубежной системой охранной сигнализации. Первым рубежом охранной сигнализации требуется блокировать:

- основную и дополнительную двери - на открывание и разрушение,
- дверной табур - на проникновение,
- оконные конструкции - на открывание и разрушение (разбитие) стекла.

Т.к. защитная решетка находится не с наружной стороны, то ее нет необходимоти дополнительно защищать охранным извещателем на открывание

и разрушение.

Извещатели для защиты дверей и тамбура объединяются в отдельный шлейф (шлейф 1). Извещатели от оконных конструкций объединяются в другой шлейф (шлейф 2) для возможности охраны окон в дневное время суток, т.к. они не являются открываемыми.

Вторым рубежом охранной сигнализации защищается объем помещения на проникновение с помощью объемных извещателей. Поскольку защищаемое помещение небольшое и имеет простую геометрическую форму, то возможно защищать весь объем помещения небольшим количеством извещателей. По сути можно обойтись одним извещателем, расположенным на потолке в углу, образованном внешней стеной с окном и стеной, противоположной дверному проему (см. рис. 1). Третьим рубежом охранной сигнализации блокируются отдельные предметы, сейфы. В рассматриваемом помещении предлагается защищать на третьем рубеже сейф с конфиденциальными документами и ПЭВМ с конфиденциальной информацией. Помещение подгруппы AII должно оборудоваться самостоятельными шлейфами охранной сигнализации. Извещатели второго и третьего рубежей подсоединяются к отдельному шлейфу 3. Т.о. имеется 3 независимых шлейфа охранной сигнализации из защищаемого помещения. Эти шлейфы в помещении подгруппы AII следует проводить по одному из следующих вариантов:

- скрытым способом в стальных трубах и металлорукавах, проложенных в полу или пластмассовых трубах, проложенных в стенах;
- скрытым способом в пластмассовых трубах или открытым способом в желобах, лотках, проложенных за подвесным потолком.

На первом рубеже охраны блокировку дверей (основной и дополнительной) и окна на открывание рекомендуется производить простейшими магнитоконтактными извещателями типа СМК. Блокировку окна на разрушение стекла рекомендуется производить извещателями омическими (фольга), поверхностными ударноконтактными извещателями типа ”Окно” или

поверхностными звуковыми извещателями типа "Стекло". Блокировку дверей (дополнительной решетчатой и основной) на разрушение рекомендуется производить омическими извещателями (провод типа НВМ, диаметром 0,18 - 0,25 мм). Для блокировки тамбура предлагается применять линейный пассивный ИК-извещатель типа "Фотон-10" с зоной обнаружения в виде плоскости, расположенной между основной и дополнительной дверьми и параллельной им. Извещатель можно разместить в правом верхнем углу дверного проема.

На втором рубеже охраны для защиты объема помещения предлагается применять пассивный оптико-электронный извещатель типа "Фотон-10" или 9981 фирмы "ADEMCO" с объемной зоной обнаружения, ультразвуковый извещатель типа "Эхо-3", комбинированный типа DT 4201, DT 4351, DT 4501 фирмы "С&Л" и им подобные. Данный извещатель можно крепить к внешней стене помещения, в котором располагается окно, недалеко от стены, противоположной входу. Извещатель следует крепить к верхней части стены. Расположение извещателя связано с тем, чтобы избежать прямого попадания солнечных лучей в извещатель.

На третьем рубеже охраны для защиты сейфа, в котором размещены конфиденциальные документы, предлагается применить емкостной извещатель типа "Пик". Для защиты ПЭВМ рекомендуется использовать поверхностный электростатический извещатель типа "Гюрза".

На рис. 4 изображены 3 шлейфа охранной сигнализации, перечислены все необходимые извещатели с указанием модельного ряда и указано распределение извещателей по шлейфам. Хотя в данной работе ПКП специально не рассматриваются, можно упомянуть о том, что в качестве ПКП здесь можно использовать "Рубин-3".

Пожарная сигнализация здесь не рассматривается. В случае необходимости можно считать, что объемный ИК-извещатель является также и пожарным, т.к. срабатывает на изменение температуры.

В соответствии с РД 78.36.003-2002 для объектов подгруппы АII рекомендованы основные характеристики, указанные в таблице 1. Камеру видеонаблюдения предлагается установить над объемным извещателем второго

Рис. 4: Распределение извещателей системы охранной сигнализации по 3-м шлейфам сигнализации. К данным шлейфам не присоединяются никакие другие извещатели от других охраняемых помещений.

Разрешение, ТВЛ, не менее	450
Чувствительности на ФЭП, лк, не хуже	0,5
Отношение сигнал/шум, дБ	50
Глубина АРУ, дБ	26
Синхронизация	внешняя

Таблица 1: Основные характеристики телевизионных камер для объектов подгруппы AII

рубежа охраны в углу комнаты. Крепить камеру можно к потолку. Сигнал от ТВК выводится из помещения по коаксиальному кабелю (РК-75-4, РК-75-6 или РК-75-9). Соответствующие максимально допустимые дальности передачи указаны в таблице 3.

Описанным требованиям к ТВК удовлетворяет, например, ТВК SpeedDome Ultra VI фирмы Sensormatic. Данное изделие является комбинацией собственно ТВК, кожуха и поворотного устройства. Камера является поворотной и в ее область обзора попадает все помещение.

Тип кабеля	Макс. дальность передачи, м
РК-75-4	50
РК-75-6	100
РК-75-9	200

Таблица 2: Максимальная дальность передачи видеосигнала по коаксиальному кабелю в метрах

Производитель	Sensormatic
Название	SpeedDome Ultra VI
Стандарт видеосигнала	PAL, цветной
Горизонтальное разрешение	более 470 ТВЛ
Минимальное освещение	0,01 лк
Объектив	асферический
Соотношение сигнал/шум	50 дБ
Видеовыход	1В, 75 Ом
Управление	SensorNet, RS-422
Габариты	⌀120×205 мм
Масса	1,2 кг

Таблица 3: Технические характеристики цветной купольной телевизионной камеры видеонаблюдения SpeedDome Ultra VI

4 Защита акустической речевой информации на объекте и противодействие утечке по оптическому каналу

Аналитическим путем проверено соответствие защищенности объекта требованиям временной методике по акустической защищенности объекта. На основе результатов, полученных в процессе оценки защищенности помещения с учетом расположения объекта, требования к акустической защищенности у существующего объекта не выполняются. В целях повышения акустической защищенности необходимо разработать предложение по защите помещения от утечки информации по вышеназванным (раздел 1) каналам.

Прежде всего, разрабатывая предложения по защите, необходимо указать на проведение специальной проверки защищаемого помещения на наличие закладных устройств с передачей снятой аудио-, фото-, видео- и др. информации по радиоканалу, линиям связи, питания и управления различных технических средств, расположенных в помещении. Для проведения данного мероприятия можно использовать дифференциальный детектор поля АРК-ДДП, сканирующий супергетеродинный приемник "AR-5000" и универсальный комплекс мониторинга технических каналов утечки информации "Крона 6000". Кроме того для решения этой задачи можно применять визуальный контроль (досмотровый комплект типа "Шмель-2"), металлодетекторы ("ВМ-12Н", "Стерх-92АР", АКА7202 и др.), нелинейные радиолокаторы ("Обь-3", "Родник-2К", "NR-900EM"), подповерхностные локаторы ("Раскан-1"), рентгенотелевизионные системы ("Шмель-90К", "Очертание - К2М", "Модуль-50"), ультразвуковые системы (томограф А1230, толщиномер А1220).

Рассмотрим защиту от акустического и виброакустического каналов утечки. Существующие ограждения обеспечивают следующие значения ослабления акустического сигнала в октавных полосах (значения приведены в дБ)(см. таблицу 4).

Конструкция	Среднегеом. частота октавной полосы, Гц							
	63	125	250	500	1000	2000	4000	8000
Железобетонная плита толщиной 300 мм (стены, пол, потолок)	44	44,5	50	58	65	69	69	69
Дверь (звукоизолирующая тяжелая)	22	24	36	45	51	50	49	56
Двойное стекло 4 мм с воздушным промежутком 200 мм	-	28	36	41	48	54	56	-

Таблица 4: Ослабление акустического сигнала ограждениями в октавных полосах, дБ

В соответствии с методикой Гостехкомиссии России оценки акустической защищенности помещения, т.к. помещение не оборудовано системами звукоусиления, то с учетом расположения защищаемого помещения относительно других помещений и улиц нормативное значение октавного коэффициента звукоизоляции составляет:

- для стен (не выходящих на улицу) и перекрытий - 46 дБ,
- для стен, выходящих на улицу, - 36 дБ,
- для окон - 36 дБ,
- для дверей - 46 дБ.

Из данной таблицы видно, что внешние стены защищены достаточно во всех октавах. Недостаточна звукоизоляция перекрытиями и внутренними стенами (необходимо добавить 2 дБ в октавной полосе 63 Гц и 1,5 дБ в полосе 125 Гц). Для повышения коэффициента звукоизоляции в нижних октавах предлагается применить гибкую плиту на относе от перекрытий и внутренних стен, что позволяет повысить коэффициент на 5-7 дБ. Окна не удовлетворяют требованиям по звукоизоляции в октавной полосе 125 Гц (и, судя по всему, в полосе 63 Гц). Здесь предлагается вместо внутреннего одинарного окна поставить окно телестудий 10-8-10 с переменными воздушными зазорами, для которого выполняются требования по звукоизоляции ($\geq$ 36 дБ) во всех октавных диапазонах. Для повышения звукоизоляции дверями предлагается укрепить внутреннюю решетчатую дверь до тяжелой звукоизолирующей двери, что повысит звукоизолирующую способность в нижних октавных полосах (63 Гц и 125 Гц) до 22 и 24 дБ соответственно. В остальных октавных полосах требования будут выполнены ($\geq$ 46 дБ). Далее предлагается соорудить в помещении большой тамбур (площадью 1,5 м х 1,5 м) со стенами в полную высоту помещения из оштукатуренных шлакоблоков толщиной 220 мм. Дверь в тамбуре предлагается вывести в сторону окна. Она должна быть двойной, тяжелой с облицовкой тамбура. Это мероприятие (возведение тамбура) уменьшит область обзора ТВК и область чувствительности объемного ИК-извещателя. Для компенсации

этого можно поставить в угол, противоположный углу расположения ТВК, еще один объемный датчик второго рубежа охраны с выводом его в шлейф 3 сигнализации.

Для звукоизоляции систем, обеспечивающих доступ воздуха в помещение, (каналов вентиляции и отопления) предлагается установить в воздуховоды глушители. Предлагается остановиться на глушителях длиной 1 м с маленькой площадью свободного сечений ($<$0,014 м^2) для небольшой ширины щели. Набор таких глушителей может обеспечить достаточную звукоизоляцию. При этом неободимо гарантировать нахождение этих глушителей в пределах контролируемой зоны.

В качестве дополнительной защиты от виброакустического канала или канала утечки с использованием модуляции излученного сигнала можно предложить использование комплекса виброакустической защиты "Барон-2" с различными вибродатчиками на стекла ("Копейка"), рамы ("Серп"), стены и двери ("Молот"). Следует отметить, что данная мера является в данном случае необязательной и носит вспомогательных характер.

Наряду со средствами обнаружения устройств звукозаписывающей аппаратуры, используемой для проведения несанкционированной записи конфиденциальных переговоров на практике эффективно используются и средства их подавления. Для этих целей могут быть использованы устройства подавления диктофонов (УПД), представляющие из себя высокочастотный генератор, излучение которого воздействует на электронную часть диктофона или радиомикрофона и нарушает режим записи, в результате чего при прослушивании вместо разговора обнаруживается запись шумового сигнала. Часто УПД монтируются в кейс (блок подавления, антенная система, система включения-выключения подавителя).

Такое конструктивное выполнение позволяет оптимально использовать его незаметно для собеседника с учетом, прежде всего ширины диаграммы направленности устройства. Диаграмма направленности должна по максимуму быть направлена на место расположения аппарата записи. В этом случае гарантируются параметры подавления.

В качестве УПД предлагается устройство электромагнитного подавле-

Рис. 5: Схема размещения устройства подавления диктофонов ”Буран 3” в области стола для переговоров

ния типа ”Буран 3”. Поскольку в помещении находится один стол, то необходимо учитывать тот факт, что размещение злоумышленника должно быть таким, чтобы он попадал в пределы диаграммы направленности устройства подавления. Устройство предлагается располагать так, как показано на рис. 5, и включать только во время проведения конфиденциальных переговоров. Технические характеристики можно найти в таблице 5.

Дальность подавления	экранированных - до 1,3 м, неэкранированных - не менее 2,5 м
Рабочие частоты	900 - 1000 МГц
Зона подавления	шаровой сектор с углом 45°, в ортогональной плоскости ширина диаграммы направленности -15°
Питание	220 В, 50Гц
Примечания	проводное дистанционное управление, имеет сертификат Гостехкомиссии России и сертификат соответствия медицинским нормам.

Таблица 5: Технические характеристики ”Буран 3”

Для защиты от утечки акустической информации по сотовому телефону помимо подавления микрофона устройством ”Буран-3” можно применить

систему блокировки сотовой связи "Мозаика", включаемую на время проведения конфиденциальных переговоров. Данная система обеспечивает блокировку сотовой связи стандартов GSM-900/1800, AMPS/DAMPS, CDMA в радиусе 3-15 м (в зависимости от близости базовой станции). Диапазон рабочих частот изделия 840-960 МГц и 1680-1920 МГц. Для блокировки стандарта NMT-450i необходимо применение модификации системы для этого стандарта - "Мозаика-NMT".

Для защиты от непосредственной утечки по оптическому каналу через окно с учетом наличия большого количества потенциальных мест, из которых можно вести оптическое наблюдение (жилые дома), предлагается использовать занавески и драпировки различных типов для экранирования на время работы с конфиденциальными документами и обработки конфиденциальной информации на ПЭВМ. В качестве варианта возможно рассмотрение применения "зеркальных" или затемненных окон с ограничением прохождения света изнутри вовне.

Для защиты от утечки по оптическому каналу за счет применения фотоаппатаруры, видеоаппаратуры в защищаемом помещении, предлагается использовать организационно-технические мероприятия, основанные на контроле людей, проходящих в помещение, на наличие содержащих металл предметов и их проверке. Особое внимание следует уделить сотовым телефонам, подавляющее большинство представителей бизнес-класса которых оснащены фото- и/или видеокамерами. Оптический канал также может функционировать на основе несанкционированного использования охранной ТВК видеонаблюдения. Предлагается отключать ТВК от линии передачи информации, управления и питания физически на время проведения конфиденциальных переговоров, работы с конфиденциальными документами на традиционных и электронных носителях. При этом устройство отключения/включения должно находиться в пределах контролируемой зоны. Эта же мера позволяет противостоять акустопреобразовательному каналу утечки от ТВК по сетям питания, управления и передачи, а также каналу утечки от закладных устройств по вышеназванным каналам. Для обнаружения закладных фото- и видеоустройств можно применять те же

мероприятия, как и для обнаружения закладных устройств съема акустической информации.

Для защиты от акустопреобразовательных каналов вследствие преобразования акустического сигнала в электрический в датчиках охранной сигнализации, а также для защиты от утечки по линиям связи сигнализации от закладных устройств, использующих эти каналы, предлагается на время ведения конфиденциальных переговоров отключать все охранные извещатели от шлейфов сигнализации. Если провести выводы от оконных охранных извещателей к шлейфу 2 в обход защищаемого помещения, то можно обеспечить охрану окон и на время проведения переговоров.

Т.к. не представляется возможным отключить на время переговоров помещение от сети электропитания, то предлагается в этом случае использовать специализированные технические средства. Устройство МП-3 (МП-1С) предназначено для защиты от утечки информации по сети питания 220 В за счет акустопреобразовательного эффекта в различных технических средствах и за счет ВЧ-навязывания. Оно обеспечивает затухание на частоте 1 кГц не менее 80 дБ. При этом предельная мощность защищаемых устройств не должна превышать 170 Вт. Питается изделие от сети 220 В.

Для подавления несанкционированной передачи данных по сети переменного тока 220 В предлагается использовать устройство защиты информации от утечки по электрической сети SP-41. Оно формирует помехи в виде цифрового шума в диапазоне 50 кГц...5МГц и амплитудой не менее 10 В в диапазоне 50 кГц...500 кГц и не менее 1 В в диапазоне 500 кГц...5МГц. При этом мощность подаваемого в сеть шумового сигнала составляет 5 Вт. Питание устройства происходит от сети 220 В. Для зашумления в более широком диапазое частот (10 кГц...1 ГГц) можно применить устройство зашумления сети питания "Соната-РС-1".

5 Защита информации в телефонных линиях и ПЭВМ на объекте

Защита средств вычислительной техники (автоматизированных рабочих мест) от снятия информации за счет побочных электромагнитных излучений и наводок осуществляется пассивными и активными способами, но в основном рассматриваются активные способы, так как ПЭВМ используется в защищаемом помещении только при проведении конфиденциальных переговоров. Средства активного подавления опасных сигналов представляют собой генераторы пространственного и линейного зашумления. Т.к. мощность побочных электромагнитных излучений мала, то генераторы широкополосных заградительных помех для пространственного зашумления рассматриваются как достаточно эффективные средства зашиты информации. Возможности более эффективного подавления опасных сигналов прицельной помехой затруднены из-за неопределенности значений их частот. Для измерения характеристик побочных электромагнитных излучений создаются автоматизированные комплексы. Примером такого комплекса может служить программно-аппаратный комплекс «Навигатор» (НПЦ Фирма «Нелк»), разработанный на базе анализатора спектра фирмы Hewlett Packard, управляемого ПЭВМ с использованием специального программного обеспечения. Комплекс обеспечивает автоматические и полуавтоматические измерения принимаемых излучений, обработку и отображение полученных результатов на экране монитора ПЭВМ. Контроль радиоэлектронной обстановки в проверяемых помещениях с возможностью накопления информации и сравнения ее с полученными ранее данными. Наиболее опасными, с точки зрения несанкционированного снятия за счет побочных электромагнитных излучений и наводок (ПЭМИН), являются мониторы компьютеров со стандартами разверток телевизионных систем. Во всех указанных случаях даже использование мощных криптографических методов защиты, информации не приводит к желаемым результатам, и только применение специальных методов и аппаратуры защиты от ПЭМИН способно устранить возникающий канал утечки информации. Такими метода-

ми являются:

1. Доработка устройств вычислительной техники с целью минимизации электромагнитных излучений (применение малоэнергетических микросхем, устройств отображения на жидких кристаллах, локальная экранировка отдельных устройств персональных компьютеров, гальваническая развязка по цепям электропитания и т.д.).

2. Электромагнитное экранирование помещений, в которых расположена вычислительная техника, а также другое электронное оборудование, используемое для обработки как аналоговой, так и дискретной информации.

3. Активное радиотехническое подавление побочных электромагнитных излучений и радиотехническая маскировка работающей аппаратуры.

Доработка устройств вычислительной техники позволяет существенно уменьшить уровень побочных электромагнитных излучений, однако полностью их не устраняет. Необходимо также отметить, что электромагнитное экранирование вносит определенный дискомфорт в работу пользователей и обслуживающего персонала, а в некоторых случаях произвести такое экранирование не представляется возможным.

Активное радиотехническое подавление и маскировка ПЭМИН были предложены Институтом радиотехники и электроники РАН и заключаются в формировании и излучении в непосредственной близости от устройств вычислительной техники широкополосного шумового сигнала с уровнем излучения, превышающим уровень информационных излучений во всем частотном диапазоне, где имеются эти излучения, а также в осуществлении наводок, подавляющих шумовые колебания в отходящие цепи коммутации.

Для осуществления электромагнитного подавления ПЭМИН разработан класс генераторов электромагнитных колебаний белого шума, издающих шумовое электромагнитное поле от десятков килогерц (кГц) до единиц гигагерц (ГГц) со спектральным уровнем излучаемого сигнала, существенно превышающем уровни естественных шумов, излучаемых средствами

вычислительной техники. Спектральная плотность излучаемого электромагнитного поля генераторами белого шума равномерно распределена по частотному диапазону зашумления и обеспечивает требуемое превышение маскирующего сигнала над побочным электромагнитным излучением в заданное число раз.

Изначально для шумового подавления и маскирования ПЭМИН в Специальном конструкторском бюро ИРЭ РАН был разработан широкополосный генератор "Шатер-4". В настоящее время различными организациями разрабатывается, изготавливается и распространяется целый класс таких приборов - широкополосные генераторы (передатчики) шумовых электромагнитных колебаний. Однако при выполнении работ по подавлению побочных электромагнитных излучений и наводок необходимо устанавливать только те изделия, которые имеют сертификат Гостехкомиссии России и удовлетворяют медико-биологическим нормам. Существует два типа изделий электромагнитного зашумления:

- генераторы объемного электромагнитного зашумления,
- генераторы локального электромагнитного зашумления.

Каждый генератор объемного электромагнитного зашумления, сертифицированный Гостехкомиссией России, обеспечивает электромагнитное зашумление помещения площадью 50 м^2. Для зашумления больших помещений необходимо устанавливать несколько таких генераторов, распределенных по площади электромагнитной защиты. Генераторы объемного электромагнитного зашумления формируют электромагнитное поле шума с поляризацией, близкой к круговой, что обеспечивает равномерное зашумление защищаемого пространства. Типичными представителями генераторов объемного электромагнитного зашумления являются: изделие "Гном", "Сфера", ГСС, "Октава", ГШ-1000, ГШ-1000М, "Баррикада", "Гром", "Волна". В качестве генераторов локального зашумления, которые встраиваются в процессорный блок персонального компьютера, рекомендовано использовать изделия: ГШ-К-1000, "Смог", "Салют". Близкое расположение генераторов электромагнитного шума к защищаемой аппаратуре, а в ряде

случаев и непосредственное включение в их блоки не оказывают мешающего и вредного воздействия на их работу. Из известных на рынке без-

Диапазон частот шумового сигнала:	10 кГц... 1 ГГц
Уровень шумового сигнала на выходных разъемах генератора в диапазонах частот: 10...150кГц 150кГц...30МГц 30...400МГц 0,4...1ГГц	 (при полосе пропускания приемника 200Гц) - $\geq$ 70 дБ (при полосе пропускания приемника 9кГц) - $\geq$ 70дБ (при полосе пропускания приемника 120кГц) - $\geq$ 75 дБ (при полосе пропускания приемника 120кГц) - $\geq$ 45 дБ
Антенны	рамочные, монтируемые в помещении в трех плоскостях
Питание	220В, 50Гц
Примечания	сертификат Гостехкомиссии РФ и сертификат соответствия медицинским нормам

Таблица 6: Технические характеристики генератора шума "Гном 3"

опасности генераторов шума был выбран генератор шума для защиты от утечки информации за счет ПЭМИН компьютеров «Гном-3». Технические характеристики изделия можно найти в таблице 6. При установке требуется произвести монтаж в помещении рамочных антенн в соответствии с требованиями руководства по эксплуатации.

Для защиты конфиденциальной информации при передаче через телефонные линии связи, а также от утечки акустической информации за счет микрофонного эффекта, режима "длинное ухо", высокочастотного навязывания, предлагается использовать телефонный модуль для комплексной защиты телефонной линии от прослушивания "Прокруст-2000". Он предназначен для защиты городской телефонной линии до АТС методом постановки активной помехи, подавляющей действие практически любых, суще-

ствующих на сегодняшний день, телефонных закладок во время разговора. В приборе реализовано запатентованное решение, позволяющее гарантированно предотвращать съем и передачу информации по телефонной линии в промежутках между телефонными переговорами. Прибор позволяет осуществлять обнаружение подключенных телефонных закладок и контролировать постоянную составляющую напряжения в телефонной линии. Защитный модуль прост в эксплуатации, практически не требует настройки пользователем, включение защиты при переговорах осуществляется нажатием одной кнопки на приборе или пульте ДУ. При необходимости можно отрегулировать уровень помехи и напряжения на линии, контроль напряжения на линии осуществляется с помощью встроенного вольтметра. Модуль обеспечивает световую индикацию режимов работы и состояния телефонной линии, а также световую индикацию пиратского использования линии в промежутках между переговорами. Документирование телефонных переговоров обеспечивается подключением звукозаписывающего устройства. Изделие имеет сертификат Гостехкомиссии РФ.

Телефонная линия во время разговора защищается на всем протяжении линии от модуля до АТС, а для гарантированной защиты линии в промежутках между переговорами организован участок телефонной линии повышенной защищенности, который располагается между защитным модулем и выносным блокиратором. Способ организации участка линии повышенной защищенности и его устройство запатентованы (Патент России 2145153).

Подавление нормальной работы телефонных закладок любых типов подключения во время переговоров осуществляется путем перегрузки входных цепей двумя активными помехами с разными физическими характеристиками. Гарантируется блокирование работы комбинированных (телефон/акустика) радиопередатчиков в режиме «акустика» (линия в режиме отбоя), как питающихся от линии, так и с автономным питанием, подключенных на участке линии повышенной защищенности. Также гарантируется блокирование проникновения сигналов от аппаратуры ВЧ-навязывания на телефонный аппарат.

Встроенное стробирующее устройство управления напряжением и током на телефонной линии блокирует нормальную работу комбинированных радиопередатчиков в режиме «телефон». Модулем обеспечивается ложное срабатывание звукозаписывающей аппаратуру системы VOX (VOR), подключенной на телефонную линию в любом месте, от модуля до АТС. Обеспечивается ложное срабатывание звукозаписывающей аппаратуры, снабженной датчиком на перепад напряжения, если она подключена на участке линии повышенной защищенности. При ложном срабатывании происходит непродуктивный расход пленки и батареи питания звукозаписывающей аппаратуры. Обеспечивается улучшенная система детектирования нелинейных элементов, подключенных к телефонной линии.

Встроенный детектор гарантированно определяет и индицирует активный, параллельный телефон даже при отключенной защите. Модуль позволяет блокировать попытки использования пиратских телефонов, подключенных на участке повышенной защищенности. Встроена автоматика временного отключения защиты для предотвращения сбоев при наборе номера. Защитный модуль легко интегрируется в конфигурацию сети офисной мини АТС. Для этой цели модуль оснащен системой дистанционного управления по телефонной линии, которая позволяет использовать число защитных модулей равное числу входящих городских линий и управлять защитой с любого телефона подключенного к внутренней мини АТС. Технические характеристики комплекса "Прокруст-2000" можно найти в таблице 7.

Заключение

Таким образом, в процессе выполнения данной работы были решены следующие задачи:

- была определена подгруппа защищаемого объекта, в котором содержится конфиденциальная информация, как АII по РД 78.36.003-2002,
- была определена степень соответствия инженерной укрепленности помещения требованиям по РД 78.36.003-2002 и сформулированы пред-

Габариты	47x172x280 мм
Условия эксплуатации	отапливаемое помещение
Максимальное поднятие постоянного напряжения на линии в режиме ”Уровень”	до 39В
Диапазон шумового сигнала в режиме ”Помеха”	50 Гц...10 кГц
Максимальная амплитуда помехи в режиме ”Детектор”	до 30 В
Напряжение на диктофонном выходе	регулируемое, до 150 мВ
Питание	сеть 220 В, 50 Гц
Потребляемая мощность	не более 10 Вт

Таблица 7: Технические характеристики ”Прокруст-2000”

ложения по повышению класса защищенности элементов конструкции до требуемого в соответствии с АII:

- стены и перекрытия с класса 2 до класса 3,
- дверные конструкции с класса 2 до класса 4,
- запирающие устройства - с класса 2 до класса 4,
- оконные проемы - с класса 1 до класса 2.

- были сформулированы требования к системе охранной сигнализации для данного объекта подгруппы АII по РД 78.36.003-2002 и выбраны конкретные модели охранных извещателей для каждого рубежа защиты:

  рубеж 1: основная и дополнительная двери на открытие - СМК, основная и дополнительная двери на разрушение - провод НВМ, дверной тамбур на проникновение - ”Фотон 10”, окно на разбитие - ”Окно”, окно на открытие - СМК;

  рубеж 2: объем - ”Фотон-10”;

  рубеж 3: сейф - ”Пик”, ПЭВМ - ”Гюрза”;

кроме того, сигнальные выводы с охранных извещателей были разведены явным образом по 3-м шлейфам сигнализации.

- были сформулированы требования к системе видеонаблюдения для подгруппы АII по ГОСТ Р51558-2000 и РД 78.36.003-2002 и предложена ТВК Sensormatic SpeedDome Ultra VI с соответствующими характеристиками и кабель РК-75-6;

- были сформулированы требования к защите конфиденциальной речевой информации от утечки по ряду каналов (см. набор каналов утечки в разделе 1) и предложены модели соответствующих технических средств защиты информации и конкретные мероприятия:

  – усиление коэффициента звукоизоляции внутренних стен и перекрытий (до 46 дБ), окон и внешних стен (до 36 дБ), дверей и глушителей на воздуховодах (до 46 дБ) в октавных полосах (пассивная защита),

  – применение ряда технических средств и проведение организационно-технических мероприятий по поиску закладных устройств различного типа (см. набор соответствующих технических средств в разделе 4),

  – применение комплекса "Буран-3" в качестве устройства электромагнитного подавления диктофонов,

  – применения устройства подавления сотовой связи "Мозаика",

  – физическое отключение линий связи, питания и управления от ТВК и охранных извещателей,

  – применение устройства МП-3 для защиты от утечки по сети электропитания за счет акустоэлектрических преобразований и ВЧ-навязывания,

  – применение устройства "SP-41" для подавления несанкционированной передачи данных по сети электропитания.

- были сформулированы требования к защите конфиденциальной информации от утечки по оптическому каналу, включающие ряд пассивных средств и методов защиты:
  - экранирование окна занавесами, затемнение окон, применение "зеркальных" окон,
  - поиск закладных устройств, передающих фото- и видеоизображение, с помощью набора технических средств (см. раздел 4) и блокировка возможных каналов передачи этой информации,
  - контроль проноса в помещение фото- и видеокамер,
  - отключение охранной ТВК на время работы с конфиденциальной информацией от линий связи, питания и управления.
- для защиты информации, передаваемой по телефонной линии, от утечки, а также для защиты акустической речевой информации от утечки по телефонной линии (в том числе для защиты от закладок типа "длинное ухо"), был предложен комплекс "Прокруст 2000";
- для защиты конфиденциальной информации, обрабатываемой на ПЭВМ, по ПЭМИН был предложен генератор шума "Гном-3".

Таким образом, была разработана комплексная система требований по защите данного объекта информатизации, в которой были учтены требования по инженерно-технической защите информации и охране объекта, а также ряд нормативно-правовых документов, изданных Гостехкомиссией России (непосредственно в части защиты информации) и МВД РФ (в части охраны).

Список литературы

[1] Д.Б. Халяпин. Защита информации. Вас подслушивают? Защищайтесь! М.: НОУ ШО "Баярд", 2004 - 432 стр.

[2] РД 78.36.003-2002. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств. МВД РФ. М., 2002

[3] РД 78.36.003-99. Рекомендации по комплексному оборудованию банков, пунктов обмена валюты, оружейных и ювелирных магазинов, коммерческих и других фирм и организаций техническими средствами охраны, видеоконтроля и инженерной защиты. Типовые варианты. МВД РФ. М., 1999

[4] ГОСТ Р 51558-2000. Системы охранные телевизионные. Общие технические требования и методы испытаний. М., 2000