Баркалов Ю.М.,
Нестеровский О.И.,
Лиходедов Д.Ю.

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СПЕЦИАЛЬНЫХ МЕРОПРИЯТИЙ

Методические рекомендации

Издано в авторской редакции
по решению методического совета института

Воронеж
Воронежский институт МВД России
2016

Авторы: Баркалов Юрий Михайлович,
394065, Россия, Воронеж, пр. Патриотов, 53. Тел.: (473) 200-52-43.
Нестеровский Олег Игоревич,
394065, Россия, Воронеж, пр. Патриотов, 53. Тел.: (473) 200-52-44.
Лиходедов Денис Юрьевич,
394065, Россия, Воронеж, пр. Патриотов, 53. Тел.: (473) 200-52-41.

E-mail: ib@vimvd.ru

Баркалов Ю.М.

Нестеровский О.И.

Лиходедов Д.Ю.

Организационно-техническое обеспечение специальных мероприятий

Методические рекомендации

Воронеж

2016

ББК 32.811

Рассмотрены и одобрены на заседании кафедры информационной безопасности. Протокол № 6 от 16 февраля 2016 г.

Рассмотрены и одобрены на заседании методического совета института. Протокол № 7 от 28 марта 2016 г.

Рецензенты:

Сячин А.В. – начальник центра информационных технологий, связи и защиты информации ГУ МВД России по Воронежской области, полковник внутренней службы;

Душкин А.В. – начальник кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России, доктор технических наук, доцент, полковник внутренней службы.

Баркалов Юрий Михайлович. Организационно-техническое обеспечение специальных мероприятий: методические рекомендации [Электронный ресурс] / Ю.М. Баркалов, О.И. Нестеровский, Д.Ю. Лиходедов. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2016. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

ISBN 978-5-88591-373-7

Методические рекомендации содержат теоретические данные, необходимые при проведении специальных мероприятий при обеспечении защиты информации, основные этапы проведения специальных мероприятий, основные понятия в области обеспечения информационной безопасности, а также описания специальных мероприятий и рекомендации по их проведению подразделениями органов внутренних дел.

Предназначены для курсантов и слушателей радиотехнического факультета, обучающихся по специальности 10.05.02 - «Информационная безопасность телекоммуникационных систем».

ББК 32.811

ISBN 978-5-88591-373-7

СОДЕРЖАНИЕ

Введение.

Одной из важнейших задач обеспечения информационной безопасности является предотвращение незаконного доступа к обрабатываемой информации. Для решения этой задачи используются комплексный подход, предназначенный для всестороннего обеспечения защиты информации. Данный подход включает в себя как контроль эффективности элементов, средств, комплексов системы защиты и безопасности информации так и организацию и проведение комплексного контроля за выполнением мероприятий защиты информации. Для проведения эффективного контроля требуется проведение специальных мероприятий направленных на выявление дестабилизирующих факторов защиты информации и определения качественных и количественных характеристик эффективности систем защиты информации. Таким образом, к специальным мероприятиям в области защиты информации следует отнести комплекс мер направленных на своевременное предотвращение угроз и выработку мер противодействия основанных на результатах разбора инцидентов в сфере информационной безопасности.

1. Основные понятия в области обеспечения безопасности информации

Составной частью любого направления деятельности, в том числе и основ защиты информации, являются определенные понятия. Естественно, содержание основных понятий определяются в соответствии с Государственными стандартами. В тематике защиты информации таким

ГОСТом является ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Этот стандарт устанавливает основные термины и определения в области защиты информации, являющиеся обязательными к применению во всех видах документации и литературы по защите информации.

Согласно ГОСТу Р 50922-2006 к основным терминам в области защиты информации относятся:

- защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;
- правовая защита информации - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;
- техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно - технических средств;
- криптографическая защита информации - защита информации с помощью ее криптографического преобразования;
- физическая защита информации - защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;
- способ защиты информации - порядок и правила применения определенных принципов и средств защиты информации;
- защита информации от утечки - защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами;
- защита информации от несанкционированного воздействия (ЗИ от НСВ) - защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
- защита информации от непреднамеренного воздействия - защита информации, направленная на предотвращение воздействия на защищаемую

информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

- защита информации от несанкционированного доступа (ЗИ от НСД) - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации;

- замысел защиты информации - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

- цель защиты информации - заранее намеченный результат защиты информации;

- система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

- политика безопасности (информации в организации) - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности;

- безопасность информации (данных) - состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;

- объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации;

- защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

- носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

- защищаемый объект информатизации - объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности;

- защищаемая информационная система - информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности;

- угроза (безопасности информации) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

- источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации;

- несанкционированное воздействие на информацию - воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

- модель угроз (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. При этом, видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ;

- техника защиты информации - средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации;

- средство защиты информации - техническое, программное, программно - техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

- средство контроля эффективности защиты информации - средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации;

- средство физической защиты информации - средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации;

- криптографическое средство защиты информации - средство защиты информации, реализующее алгоритмы криптографического преобразования информации;

- оценка соответствия требованиям по защите информации - прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации;

- лицензирование в области защиты информации - деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с

установленными требованиями и выдаче разрешения на выполнение этих работ;

- сертификация на соответствие требованиям по безопасности информации - форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;
- специальное исследование (объекта защиты информации) - исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;
- специальная проверка - проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств;
- эффективность защиты информации - степень соответствия результатов защиты информации цели защиты информации;
- требование по защите информации - установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации;
- показатель эффективности защиты информации - мера или характеристика для оценки эффективности защиты информации;
- норма эффективности защиты информации - значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

В дополнение к рассмотренным определениям необходимо учитывать, что к объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации. В частности, для подразделений ОВД типовыми объектами защиты являются:

- выделенное помещение, в котором проводятся совещания по вопросам, содержащим сведения, составляющие государственную тайну;
- автоматизированная система, предназначенная для работы со сведениями, составляющими государственную тайну.

2. Утечка информации по техническим каналам

Применительно к объектам защиты подразделений ОВД злоумышленник потенциально может реализовать две основных возможности получения защищаемой информации, а именно:

- реазиловать технические каналы утечки информации;
- осуществить несанкционированный доступ к информации.

Под техническим каналом утечки информации (ТКУИ) понимается совокупность объекта разведки, средства разведки, среды распространения сигнала. Также верным будет определение: ТКУИ - это несанкционированный перенос защищаемой информации от источника к злоумышленнику.

Структурная схема ТКУИ представлена на рис. 1.

Рис. 1 Структурная схема ТКУИ

По физической природе возникновения ТКУИ, специфичные для подразделений ОВД, подразделяются на:

- акустические ТКУИ;
- каналы побочных электромагнитных излучений и наводок (ПЭМИН);
- видовые ТКУИ.

Акустические ТКУИ.

Источником образования акустического канала утечки информации являются вибрирующие, колеблющиеся тела и механизмы, такие как голосовые связки человека, движущиеся элементы машин, телефонные аппараты, системы звукоусиления и т.д.

Классификация акустических каналов утечки информации в зависимости от их физических особенностей представлена на рис. 2.

Распространение звука в пространстве осуществляется звуковыми волнами. Упругими, или механическими, волнами называются механические возмущения (деформации), распространяющиеся в упругой среде. Тела, которые, воздействуя на среду, вызывают эти возмущения, называются источниками волн. Упругая волна является продольной и связана с объемной деформацией упругой среды, вследствие чего может распространяться в любой среде - твердой, жидкой и газообразной.

Когда в воздухе распространяется акустическая волна, его частицы образуют упругую волну и приобретают колебательное движение, распространяясь во все стороны, если на их пути нет препятствий. В условиях помещений или иных ограниченных пространств на пути звуковых волн возникает множество препятствий, на которые волны оказывают переменное давление (двери, окна, стены, потолки, полы и т.п.), приводя их в колебательный режим. Это воздействие звуковых волн и является причиной образования акустического канала утечки информации.

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата, акустические каналы утечки информации также можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

Воздушные каналы.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны. Микрофоны объединяются или соединяются с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками. Перехваченная информация может передаваться по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн).

Вибрационные каналы.

В вибрационных (структурных) каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

Электроакустические каналы.

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические. Перехват акустических колебаний осуществляется через ВТСС, обладающие "микрофонным эффектом", а также путем "высокочастотного навязывания".

Оптико-электронный канал.

Оптико-электронный (лазерный) канал утечки информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол, окон, картин, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация.

Параметрические каналы.

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ (технические средства приема, обработки, хранения и передачи информации) и ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом.

Каналы побочных электромагнитных излучений и наводок.

Возникновение угрозы безопасности информации по каналам ПЭМИН возможно благодаря перехвату техническими средствами побочных (не связанных с прямым функциональным значением элементов информационной системы) электромагнитных полей и электрических сигналов, несущих информацию, возникающих при обработке информации техническими средствами информационной системы.

К техническим средствам, представляемым вероятным источником утечки информации по каналам ПЭМИН относятся:

- электронная и электрическая оргтехника;
- средства и системы телефонной, телеграфной (телетайпной), директорской, громкоговорящей, диспетчерской, внутренней, служебной и технологической связи;
- средства и системы звукоусиления, звукозаписи и звуковоспроизведения;
- устройства, образующие дискретные каналы связи: абонентская аппаратура со средствами отображения и сигнализации, аппаратура повышения достоверности передачи, каналообразующая и т.п.;
- аппаратура преобразования, обработки, передачи и приема видеоканалов, содержащих факсимильную информацию;
- средства и системы специальной охранной сигнализации (на вскрытие дверей, окон и проникновение в помещение посторонних лиц), пожарной сигнализации (с датчиками, реагирующими на дым, свет, тепло, звук);
- система звонковой сигнализации (вызов секретаря, входная сигнализация);
- контрольно-измерительная аппаратура;
- средства и системы кондиционирования (датчики температуры, влажности, кондиционеры);

- средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители системы радиовещания и оповещения, радиоприемники и телевизоры);

- средства и системы часофикации (электронные часы, вторичные электрочасы);

- средства и системы электроосвещения и бытового электрооборудования (светильники, люстры, настольные и стационарные вентиляторы, электронагревательные приборы, холодильники, бумагорезательные машины, проводная сеть электроосвещения).

Значения частот, на которых наводятся опасные сигналы, зависят от вида аппаратуры и располагаются в диапазоне от сотен герц до десятков гигагерц. Амплитуда наводок зависит от расстояния между источниками излучения и устройствами, которые подвергаются воздействию таких излучений, расстоянием параллельного пробега и значением затухания, а так же величиной напряжения сигнала в линии и уровнем помех.

Источниками опасных сигналов могут быть участки, которые охвачены случайными магнитными и емкостными связями. Например, монтажные колодки, разъемы блоков, контакты переключателей и реле для коммутации выходных линий и др.

Утечка информации по каналам ПЭМИН характеризуется рядом параметров, основными из которых являются:

- отношение " сигнал/шум";

- отношение напряжения опасного сигнала к напряжению шумов в полосе частот опасного сигнала.

Возникновение рассматриваемых технических каналов утечки возможно благодаря:

- гальваническим связям (способствующие получению электрического тока путем химических реакций) соединительных линий основных технических средств и систем (ОТСС) с линиями второстепенных технических средств и систем (ВТСС) и посторонними проводниками;

- наводкам ПЭМИ ОТСС на соединительные линии ВТСС и посторонние проводники;

- наводкам ПЭМИ ОТСС на цепи электропитания и заземления ОТСС;

- просачиванию сигналов в цепи электропитания и заземления ОТСС;

- ПЭМИ элементов ОТСС;

- ПЭМИ на частотах работы высокочастотных генераторов ОТСС;

- ПЭМИ, возникающие вследствие паразитной генерации в элементах ОТСС;

- высокочастотному облучению ОТСС;

- внедрению закладных устройств.

Способы перехвата информации, обрабатываемой ОТСС, представлены на рис. 3.

Рис. 3. Способы перехвата информации, обрабатываемой ОТСС

ПЭМИ элементов ОТСС. В определенных ОТСС (системы звукоусиления) электрический ток выступает носителем информации, его параметры (значение силы тока, напряжения, частоты и фазы) зависимы от речевого информативного сигнала. В процессе протекания тока по токоведущим элементам ОТСС и линиям в окружающем их пространстве возникает переменное электромагнитное поле. Таким образом, элементы ОТСС рассматриваются в качестве излучателей электромагнитного поля, изменяющегося аналогично опасному сигналу (т.е они промодулированы).

ПЭМИ на частотах вещания высокочастотных генераторов (задающих, тактовой частоты, измерительных приборов, гетеродинов устройств радиоприема). На некоторых элементах, всходящих в состав генераторов, могут наводиться электрические сигналы под действием электромагнитных колебаний. (В этом случае принимать магнитное поле будут катушки индуктивности в колебательных контурах, дроссели в цепях электропитания, а электрическое - провода высокочастотных цепей). Наведенные сигналы будут способствовать возникновению непреднамеренной модуляции собственных высокочастотных, излучаемых в окружающую среду, колебаний генераторов.

ПЭМИ, возникающие вследствие паразитной генерации в элементах ОТСС. Такая генерация имеет место быть по причине случайных преобразований отрицательных обратных связей в положительные, что

приводит к изменению режима работы усилителя (зачастую при перегрузке): переходу к автогенерации сигналов, иными словами - к самовозбуждению. Сигнал на частотах самовозбуждения модулируется информационным сигналом.

Наводки в токопроводящих элементах возникают из-за электромагнитного излучения ОТСС, а также по причине образования индуктивных и емкостных связей между ними. Соединительные линии ВТСС представляют собой случайные антенны, служащие областью распространения опасного сигнал, который в итоге затухает. Коэффициент затухания можно вычислить, исходя из данных об отрезке расстояния от места подключения средства разведки к случайной антенне до объекта ОТСС и частоты ПЭМИ.

«Просачивание» сигналов в цепи электропитания возникает при внутренних паразитных емкостных и индуктивных связях выпрямительного устройства блока питания ОТСС. Среднее значение потребляемого тока в оконечных каскадах усилителей зависит от амплитуды информационного сигнала, это оказывает неравномерную нагрузку на выпрямитель и изменяет уровень потребляемого тока пропорционально изменению информационного сигнала.

«Просачивание» информационных сигналов в цепи заземления. Помимо проводников заземления гальванической связью с землей обладают проводники, которые выходят за территорию контролируемой зоны (КЗ) (например, экраны кабелей, металлические трубы отопления и водоснабжения, нулевой провод сети электропитания, железобетонная арматура). Перечисленные проводники в совокупности с заземляющим устройством организуют систему заземления, которая подвержена наводкам опасно сигнала. Так же на определенном участке грунта, в который входит заземляющее устройство, образуется электромагнитное поле, оно также может быть использовано для получения опасного сигнала.

Существуют так же активные способы перехвата опасного сигнала, например способ, в процессе которого ОТСС облучают высокочастотным сигналом большой мощности. Это процесс высокочастотного облучения. Излучаемый сигнал воздействует на нелинейные элементы ОТСС и, будучи модулированным, переизлучается, затем его принимает средство разведки и в последствие его детектируют.

Наиболее известным из активных способ перехвата любого вида информации является скрытное внедрение закладочных устройств. В рассматриваемом техническом канале утечки закладки реализуются в виде генераторов, чье излучение модулируется опасным сигналом и передается по радиоэфиру.

Регистрация и фиксация ПЭМИН осуществляется с целью перехвата, а также изменения информации, циркулирующей в технических средствах, обрабатывающих информацию.

Для регистрации ПЭМИН применяется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Кроме этого, перехват ПЭМИН реализуется с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации, например простейший телефон.

Регистрация ПЭМИН может производиться с использованием аппаратуры следующих видов:

- стационарной аппаратурой, размещаемой в близлежащих строениях (зданиях) с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратурой - физическими лицами в непосредственной близости от информационной системы;
- автономной автоматической аппаратурой, скрытно устанавливаемой физическими лицами в непосредственной близости от информационной системы.

Используя характеристики приемного устройства и антенной системы средства разведки, можно рассчитать допустимое (нормированное) значение напряженности электромагнитного поля в некоторой точке размещения средства разведки. На данном расстоянии отношение "информационный сигнал/помеха" на входе приемного устройства будет равно некоторому значению, при котором еще возможно обнаружение средством разведки информационных сигналов.

Следовательно, можно говорить о территориальной характеристике (пространство/зона) вокруг ОТСС, пределах которой возможен перехват средством разведки побочных электромагнитных излучений ОТСС с требуемым качеством. В нормативно-методической литературе вводят понятие зоны 2.

Зоной 2 (R2) является пространство вокруг ОТСС, в пределах которого напряженность электромагнитного поля превышает допустимое (нормированное) значение.

Таким образом, для возникновения электромагнитного канала утечки информации необходимо выполнение двух условий:

- расстояние от ТСПИ до границы контролируемой зоны должно быть менее зоны R2;
- за пределами зоны R2, в пределах зоны R2 возможно размещение портативных (переносимых, перевозимых, стационарных) средств разведки ПЭМИН.

Схема перехвата побочных электромагнитных излучений ОТСС представлена на рис. 4.

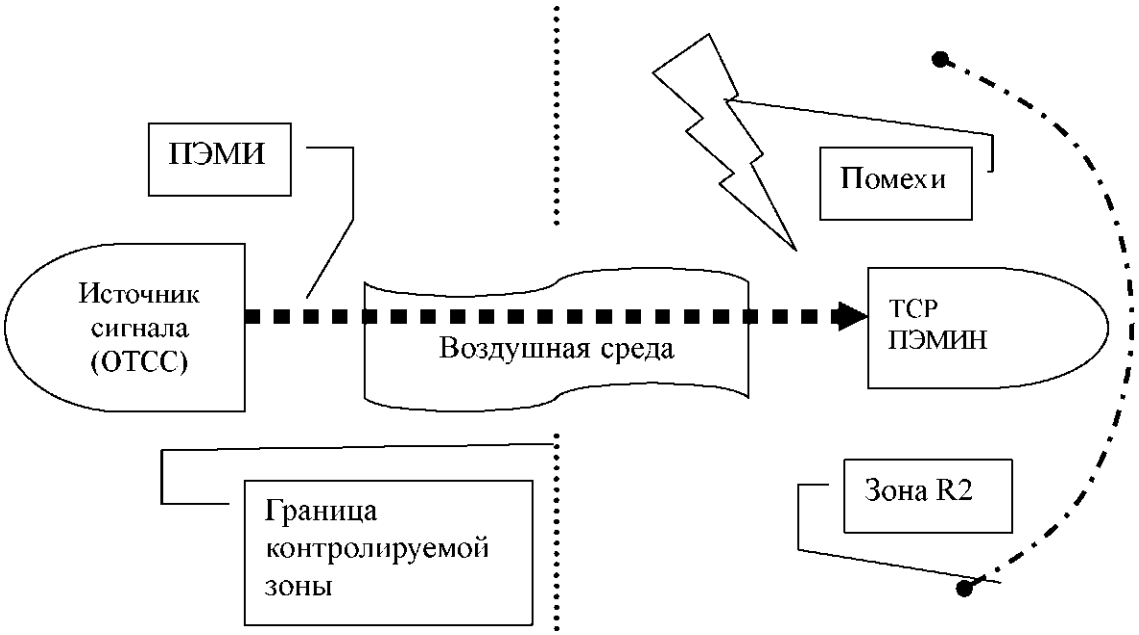


Рис. 4. Схема перехвата побочных электромагнитных излучений ОТСС

Самым часто встречаемым в любом подразделении ОВД устройством, излучающим опасные сигналы, является ПЭВМ. Следует помнить, что работающий компьютер излучает на всех частотах. Говоря об излучении монитора, можно отметить, что даже если он будет установлен корректно с точки зрения безопасности (его нельзя будет рассмотреть сторонним лицам), излучаемый им световой поток, многократно отраженный от ограждающих

конструкций, включая стены и потолок, поддается перехвату благодаря использованию современных технических разведывательных средств.

Кроме того, в оптическом диапазоне вещают светодиодные индикаторы режимов работы компьютера. Светодиоды обладают малой инерционностью, и модулируют световой поток, а так же наводки от элементов, находящихся в системном блоке до сотен мегагерц. Такие сигналы в последствие так же могут быть детектированы специальной аппаратурой для получения информационного сигнала.

Особенно чувствительны к перехвату видеотерминалы. Перехваченный сигнал достаточно просто интерпретировать, отобразив информацию на дисплее разведки. Не следует забывать, что не только излучение монитора представляет собой канал утечки защищаемой компьютерной информации. Электромагнитные излучения также испускаются принтерами, накопителями на магнитных дисках, графопостроителями и каналами сетей связи ЭВМ.

Сигналы для получения изображения, формируются в видеокарте и передаются на монитор по кабелю. Таким образом, можно перехватить видовую информацию без перехвата излучения самого экрана.

Кроме того, сигналы, которые излучает клавиатура, могут быть также исследованы, например, для вычисления пароля. Так же имеет место быть интерес к документам, распечатанным на принтере. Следует сказать, что

информация в этих устройствах передается в виде последовательного кода, параметры которого известны, так как стандартизированы.

Дальности обнаружения радиоизлучений, образованных составными элементами стандартного компьютера, представлены в таблице 1.

Таблица 1

Дальность радиоизлучений составных элементов стандартного компьютера

Блок ПЭВМ	Расстояние излучения поля, м	
	электромагнитного	электрического
Системный блок	2 - 40	1 - 30
Дисплей	25 - 120	10 - 55
Принтер	5 - 35	10 - 50
Клавиатура	15 - 50	15 - 30

Электромагнитное поле, создаваемое персональным компьютером, имеет сложный спектральный состав в диапазоне частот от единиц Гц до тысяч МГц. Взаимосвязь электрической и магнитной составляющих ЭМП достаточно неоднородна, поэтому оценка электрического и магнитного полей производится раздельно. Наличие в помещении нескольких компьютеров со вспомогательной аппаратурой и системой электропитания создает неравномерное распределение полей в помещениях.

Таким образом, можно говорить, что возможными режимами обработки информации, при которых происходит значительное излучение, характерными для типового средства вычислительной техники являются:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на накопители на магнитных носителях;
- чтение информации с накопителей на магнитных носителях;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства - принтеры, плоттеры;
- запись данных от сканера на магнитный носитель (ОЗУ).

Видовые ТКУИ.

Наряду с информацией, обрабатываемой в ОТСС и речевой информацией, важную роль играет видовая информация, получаемая техническими средствами в виде изображений объектов или документов. В зависимости от характера информации можно выделить следующие способы ее получения:

- наблюдение за объектами;
- съемка объектов.

Наблюдение за объектами. В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные

технические средства. Для наблюдения днем - оптические приборы (монокуляры, подзорные трубы, бинокли, телескопы и.т.д.), телевизионные камеры, фотографические камеры, для наблюдения ночью - приборы ночного видения, тепловизоры. Для наблюдения с большого расстояния используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния - камуфлированные скрытно установленные телевизионные камеры. Причем изображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

Съемка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съемки объектов используются телевизионные и фотографические средства. При съемке объектов, также как и при наблюдении за ними, использование тех или иных технических средств обусловлено условиями съемки и временем суток.

В зависимости от состава защищаемого объекта информатизации рассмотренные группы каналов могут как присутствовать, так и отсутствовать.

Например, если речь идет о защите «классической» автоматизированной системы (АС) в составе: персональной электронно-вычислительной машины (ПЭВМ), принтера,

3. Несанкционированный доступ к информации

Одной из возможностей злоумышленников получить защищаемую информацию является несанкционированный доступ к ней.

Несанкционированный доступ к информации может включать неавторизованное пользование информацией системы и активную инфильтрацию.

Неавторизованное пользование предполагает возможность ознакомления с информацией, хранимой в системе, и использование ее в своих целях.

Под активной инфильтрацией информации подразумеваются такие действия, как просмотр чужих файлов через удаленные терминалы, маскировка под конкретного пользователя, физический сбор и анализ файлов на различных носителях.

Преднамеренные попытки проникновения в автоматизированные системы обработки данных могут быть как активными, так и пассивными.

Пассивное проникновение — это подключение к линиям (коммуникациям) связи или перехват электромагнитных излучений этих линий или ОТСС в любой точке доступа к ним лицом, не являющимся пользователем.

Активное проникновение — прямое использование информации из файлов информационно-телекоммуникационной системы и ее элементов, в том числе с использованием ОТСС, носителей информации.

При активном проникновении обычно могут использоваться следующие процедуры доступа:

- использование известного способа доступа к системе или ее элементам с целью задания запрещенных вопросов, обращения к файлам, содержащим интересующую информацию;

- маскировка под истинного пользователя после получения характеристик (идентификаторов) доступа;

- использование служебного положения — незапланированного просмотра (ревизии) информации на файлах.

Активное проникновение в системы обработки информации может осуществляться скрытно с использованием следующих наиболее характерных приемов проникновения:

- использование точек входа, установленных в системе программистами, обслуживающим персоналом или точек, обнаруженных при проверках цепей системного контроля;

- подключение к системам телекоммуникаций специального терминала, обеспечивающего вход в систему путем пересечения линий связи законного пользователя с ТСОИ и последующим восстановлением связи по типу ошибочного сообщения, а также в момент, когда законный пользователь не проявляет активности, но продолжает занимать канал связи;

- аннулирование сигнала пользователя о завершении работы с системой и последующее продолжение работы от его имени;

- неавторизованная модификация хранящейся в системе информации, затрудняющая получение пользователем доступа к информации, ему принадлежащей.

Основными способами НСД являются:

- непосредственное обращение к объектам доступа;

- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

- модификация средств защиты, позволяющая осуществить НСД;

- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

4. Комплексность в защите информации

Решение проблемы обеспечения информационной безопасности предполагает реализацию комплексной защиты информации.

Комплексная защита информации — соединение в единое целое отдельных элементов, механизмов, процессов, явлений, мероприятий, мер и программ ЗИ, их взаимосвязей, способствующих:

- реализации целей защиты;

- реализации концептуального подхода защиты;

- реализации временного функционирования системы защиты;

- обеспечению структурного построения системы защиты.

Таким образом, основное положение современной постановки проблемы формулируется как обеспечение комплексной защиты

информации, предполагающее комплексность целевую, концептуальную, временную и структурную.

Целевая комплексность означает, что защита осуществляется по всем показателям информационной безопасности и всей совокупности факторов, влияющих на нее, а системы защиты информации должны строиться для достижения следующих целей:

1) обеспечения физической целостности защищаемой информации, т.е. заданной синтаксической ее структуры;

2) обеспечения логической целостности, т.е. семантических характеристик информации и установленных взаимосвязей между ее элементами;

3) обеспечения доверия к информации в прагматическом плане, т.е. предупреждения несанкционированной ее модификации с изменением или без изменения синтаксических или семантических характеристик;

4) предупреждения несанкционированного получения защищаемой информации лицами или программами (процессами), не имеющими на это специальных полномочий, т.е. обеспечения установленного статуса ее секретности (конфиденциальности);

5) предупреждения несанкционированного копирования (размножения) информации, объявленной чьей-либо собственностью;

6) защиты от демаскирования, т.е. скрытия назначения, архитектуры, технологии и самого факта функционирования системы обработки информации;

7) защиты личности, общества, государства, в т.ч. их информационных ресурсов, информации, информационных систем от воздействия информации, наносящей ущерб, внешних и внутренних угроз.

Применительно к конкретному объекту защиты могут быть рассмотрены только некоторые из перечисленных целей и сформулированы дополнительные цели (с учетом особенностей объекта защиты).

Временная комплексность предполагает непрерывность осуществления мероприятий по защите информации, как в процессе непосредственной ее обработки, так и на всех этапах жизненного цикла информационно-телекоммуникационных систем. Это предполагает организацию и обеспечение целенаправленного управления всей совокупностью способов, средств и мероприятий ЗИ на различных этапах жизненного цикла системы обработки информации.

Комплексность структурная предполагает использование различных средств защиты. Для достижения различных целей комплексной защиты информации необходимо предусмотреть адекватные по содержанию и достаточные по количеству способы и средства защиты элементов, отдельных образцов ТСОИ и в целом любой системы обработки информации.

Выбор множества и разнообразия средств защиты обычно осуществляется на основе содержания конкретных задач защиты, множества

потенциальных угроз, дестабилизирующих факторов и причин, их порождающих, способов противодействия дестабилизирующим факторам и угрозам с учетом обеспечения заданных требований и показателей информационной безопасности. При этом выбор способов осуществляется с учетом обеспечения рассмотренных выше целей комплексной защиты информации или защиты системы от воздействий разрушающей информации.

Концептуальная комплексность предполагает, что потребности, возможности и условия защиты информации должны органически учитывать аспекты системного подхода, выраженные в целевых, временных структурных положениях защиты, условиях обеспечения заданной защиты, возможностях реализации, основных принципах и направлениях концепции развития информационно-телекоммуникационных систем и их компонентов.

Основная сущность концептуального подхода заключается:

— в системном учете совокупности внешних факторов (воздействий средств иностранных технических разведок, радиоэлектронной борьбы, обычного и высокоточного вооружения, физико-географических условий, взаимодействующих систем), внутренних особенностей информационно-телекоммуникационных систем, существенно влияющих на защиту информации;

— в разработке общей концепции защиты информации, позволяющей решить наиболее полное множество частных задач защиты;

— в разработке полного множества моделей защиты информации, учитывающих реализацию рассмотренного множества целей защиты;

— в использовании формальных и неформальных методов моделирования сложных систем защиты информации и процессов их функционирования.

В обобщенном виде содержание комплексной защиты в современных системах ее обработки представлено в табл. 2.

На основе рассмотренных положений комплексной защиты информации можно представить структуру и общее содержание концепции комплексной ЗИ, являющиеся основой для разработки унифицированных защищенных технологий обработки информации.

Таблица 2

Содержание комплексной защиты информации

КОМПЛЕКСНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ

КОМПЛЕКСНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ
1. ЦЕЛЕВАЯ
а) обеспечение маскировки (скрытия) назначения системы б) обеспечение маскировки (скрытия) архитектуры системы в) обеспечение маскировки (скрытия) технологии функционирования системы г) обеспечение физической целостности информации д) обеспечение логической целостности информации е) предупреждение несанкционированной модификации информации ж) предупреждение несанкционированного получения информации з) предупреждение несанкционированного размножения информации
2. ВРЕМЕННАЯ
а) обеспечение текущей защиты б) обеспечение защиты на заданном интервале времени в) обеспечение защиты на всех этапах жизненного цикла
3. СТРУКТУРНАЯ
а) защита информации в элементах и отдельных средствах б) защита информации в отдельно взятой системе обработки информации в) защита информации в системах обработки информации страны, региона, ведомства
4. КОНЦЕПТУАЛЬНАЯ
а) комплексный учет концепций развития и использования современных средств обработки информации б) учет аспектов системности подхода в) комплексный учет всех факторов, влияющих на защиту г) комплексный учет условий и возможностей обеспечения и реализации защиты д) реализация полного множества моделей и методов решения задач защиты информации

3. Мероприятия по обеспечению безопасности информации

В соответствии с действующими нормативными и методическими документами выделяют следующие виды защиты информации:

- правовая защита информации (защита информации правовыми методами);

- техническая защита информации (защита информации с применением технических, программных и программно - технических средств);

- криптографическая защита информации (защита информации с помощью ее криптографического преобразования);

- физическая защита информации (защита информации путем применения организационных мероприятий).

Для реализации всей совокупности видов защиты информации применяются следующие группы мероприятий:

- организационные;

- технические;

- организационно-технические.

Данные группы мероприятий разрабатываются для конкретных объектов защиты. При этом, разрабатываемые комплексы мероприятий ориентированы как на защиту информации от утечки по техническим каналам, так и на защиту от несанкционированного доступа.

Организационные мероприятия включают в себя непосредственно организацию защиты информации, регламентацию деятельности по защите информации.

Организационные меры подразделяются:

- разовые (такие меры, которые проводятся однократно и повторяются только тогда, когда имеется полный пересмотр принятых решений);

- мероприятия, которые проводятся при реализации или возникновении установленных изменений в объекте информатизации, называются периодически проводимыми (через назначенное время) мероприятиями;

- постоянно (непрерывно или дискретно в любые моменты времени) проводимые мероприятия.

К типовым организационным мероприятиям относятся:

- организацию пропускного режима и охрана территории;

- организация работы с сотрудниками (подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.);

- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей защищаемой информации, их учет, выполнение, возвращение, сбережения и нейтрализации;

- организацию использования технических средств сбора, обработки, накопления и хранения защищаемой информации;

- организацию работы по анализу внутренних и внешних угроз защищаемой информации и выработке мер по обеспечению ее защиты;

- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, сбережения и нейтрализации документов и технических носителей.

Технические мероприятия предполагают использование технических средств для защиты информации на объекте информатизации. Технические мероприятия, применительно к ТКУИ, направлены на закрытие каналов

утечки информации путем снижения уровня информационных сигналов или уменьшением отношения сигнал/шум в местах возможного размещения портативных средств разведки или их датчиков до величин, обеспечивающих невыполнимость выделения информационного сигнала средством разведки. Технические мероприятия могут быть направлены на реализацию как пассивной, так и активной защиты.

Пассивная защита заключается, в общем случае, в снижении уровней сигналов, соизмеримых с естественными шумами (безх воздействия на средство разведки злоумышленника).

Активная защита предполагает, в общем случае, скрытие информационных сигналов за счет постановки активной помехи.

Естественно, наиболее эффективной будет являться комбинированная защита - уменьшение уровней излучения до заданных значений с одновременным использованием и пассивной, и активной защиты.

К типовым техническим мероприятиям относятся:

- локализация излучений за счет использования генераторов шума;
- направленное зашумление мест возможного размещения средств разведки злоумышленника.

Естественно, данные общие технические мероприятия необходимо конкретизировать под конкретный объект защиты.

Организационно-технические мероприятия предполагают использование различных технических средств для реализации тех или иных организационных моментов защиты информации.

Естественно, большинство из реализуемых на объекте защиты мероприятий целесообразно отнести к данной категории, поскольку на настоящем уровне развития техники и технологий технические средства используются практически во всех видах деятельности.

Примером организационно-технических мероприятий могут служить:

- организация пропускного режима с использованием системы электронных ключей доступа как на территорию подразделения, так и в конкретные помещения;
- применение различного рода генераторов шума в соответствии с инструкцией пользователю аттестованного по требованиям безопасности информации объекта информатизации.

Необходимо отметить, что в соответствии с законодательством Российской Федерации для защиты информации могут применяться только сертифицированные средства защиты.

Под сертификацией продукции по требованиям безопасности информации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа-сертификата и знака соответствия с определенной степенью достоверности подтверждается, что продукция соответствует:

— требованиям государственных стандартов или иных нормативных документов, утвержденных Советом Министров — Правительством

Российской Федерации (для продукции, используемой при обработке, хранении или передаче по каналам связи информации, содержащей сведения, составляющие государственную тайну);

— требованиям государственных или отраслевых стандартов, иных нормативных документов, утвержденных Советом Министров — Правительством РФ или ФАПСИ (для продукции, используемой при обработке, хранении или передаче по каналам связи конфиденциальной информации, не содержащей сведений, составляющих государственную тайну).

При проведении сертификации продукции подтверждается соответствие ее требованиям безопасности информации.

Система предусматривает сертификацию технических, программно-технических, программных средств, систем, сетей вычислительной техники как законченной научно-технической продукции, средств защиты и контроля эффективности защиты по требованиям безопасности информации.

Испытания сертифицируемой продукции проводятся в аккредитованных испытательных лабораториях (центрах).

Основные принципы, организационные структуры системы сертификации продукции по требованиям безопасности информации, а также правила проведения сертификаций этой продукции предусматриваются Законами «О стандартизации», «О сертификации товаров и услуг», проектом положения «О сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации», разработанными по рекомендациям ФСТЭК России.

Система сертификации продукции по требованиям безопасности информации направлена, в основном:

- на обеспечение прав собственника и владельца информации, владельца объекта информатизации;
- сохранение информации, обрабатываемой на объектах информатизации, в тайне;
- исключение несанкционированного искажения или уничтожения информации.

К сертифицированным средствам защиты информации от утечки по техническим каналам относятся:

- защита от утечки по каналам ПЭМИН: ГШ-1000м, ГШ-2500 и др.
- защита от утечки по акустическим ТКУИ: «Барон», «Соната-АВ», «Стена-105», «Хаос», «Соната-Р2» и т.д.

4. Контроль эффективности мероприятий по защите информации

Одной из составных частей процесса защиты информации является контроль эффективности мероприятий по защите информации. Контроль в данном случае - это способ убедиться в эффективности принимаемых мер защиты.

Контроль эффективности мероприятий по защите информации осуществляется как самими пользователями защищаемой информации, так и другими специалистами, уполномоченными для ведения контроля.

Для технических каналов утечки информации может использоваться методический подход, основанный на нормировании, то есть в рамках реализации данного подхода осуществляется регистрация определенных параметров технического канала утечки информации и проводится их сравнение с нормированными значениями указанных параметров. По результатам сравнения принимается решение о эффективности или неэффективности мероприятий по защите информации.

При этом существует три метода технического контроля:

- инструментальный;
- инструментально-расчетный;
- расчетный.

Инструментальный контроль предполагает полноценное моделирование исследуемого ТКУИ. Данный метод имеет наибольшую по сравнению с другими достоверность.

Инструментально-расчетный контроль предполагает использованием математической модели ТКУИ, при этом часть параметров ТКУИ подлежит измерению в ходе контроля.

Расчетный метод контроля предполагает использованием математической модели ТКУИ, при этом данные о параметрах ТКУИ определяются на основе ранее полученных результатов. Измерения при данном методе контроля не проводятся.

Для оценки эффективности защиты информации от несанкционированного доступа таким же подходом мы воспользоваться не можем (за исключением частных случаев, например, проверки длины пароля), поэтому в данном случае необходимо проводить более глубокий анализ систем защиты информации.

Оформление отчетных документов является неотъемлемой частью проведения контроля и осуществляется по формам, установленным действующими нормативными документами. Они включают в себя данные измерений и расчетов для контрольных точек, в которых проводились измерения, а также заключение о выполнении/невыполнении соответствующих требований по защите информации.

5. Технические средства, используемые при проведении специальных мероприятий в области обеспечения информационной безопасности.

Программно-аппаратный комплекс «Спрут-мини А» предназначен для оценки эффективности защиты речевой информации. В состав комплекс входят (Рис.5.):

1. управляющая ПЭВМ;

2. программное обеспечение управления аппаратурой акустического контроля и обработки НЧ-сигналов (один CD);

3. многоканальный сигнальный концентратор «Спрут-М3»;

4. блок формирования тестовых акустических сигналов «Спрут-Г3» с акустической системой;

5. измерительный микрофон с принадлежностями;

6. вибродатчик (акселерометр) с принадлежностями;

7. токосъемники.

Комплекс контроля эффективности защиты речевой информации «Спрут-мини» предназначен для проверки выполнения норм эффективности защиты речевой информации от утечки по акустическому, виброакустическому каналам, а также за счет НЧ наводок на токопроводящих элементах ограждающих конструкций, электроакустических преобразований в линиях ТСПИ и за счет побочных электромагнитных излучений от технических средств в речевом диапазоне.

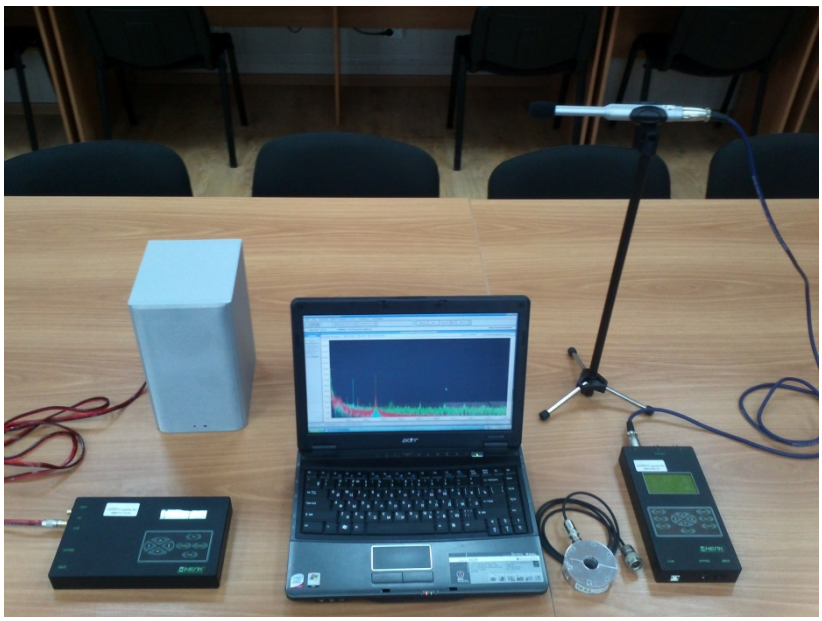


Рис.5. Комплекс «Спрут-мини А».

Комплекс обеспечивает измерение акустического давления, виброускорения, а также уровней сигналов НЧ наводок на токопроводящих элементах ограждающих конструкций, электроакустических преобразований в линиях ТСПИ и побочных электромагнитных излучений от технических средств в речевом диапазоне.

Основные технические характеристики

Комплекс функционирует в централизованном и автономном режимах и позволяет производить спектральный и октавный анализ измеряемых сигналов.

Он обеспечивает проведение измерений в диапазоне частот от 20 до 20000 Гц.

Диапазон измеряемых уровней:

звукового давления – 10–105 дБ;
виброускорений – 5·10-5–1 м/с2;
напряженности электрического поля – 10-105 мкВ/м;
напряженности магнитного поля – 0,2-104 мкА/м;
напряжений наведенного электрического сигнала - 5·10-2–103 мкВ.
Погрешность измерения, не более:
уровней звукового давления – 0,7 дБ;
виброускорений – 10-5 м/с2;
напряженности электрического поля – 2 мкВ/м;
напряженности магнитного поля – 4·10-2 мкА/м;
наведенного электрического сигнала – 10-2 мкВ;
частоты (в режиме спектрального анализа, f >150 Гц) – 2%.

Диапазон уровней звукового давления тестового сигнала на расстоянии 1 м от источника (блок формирования тестовых акустических сигналов с акустической системой) – не менее 65-90 дБ.

Время развертывания (свертывания) – не более 20 мин.

Принцип работы.

В комплекс входят серийные электронно-вычислительные и измерительные средства, функционирование которых обеспечивается при помощи специального математического программного обеспечения (СМПО).

Набор датчиков (входных преобразователей) комплекса обеспечивает преобразование измеряемых физических величин (виброускорения, уровня звукового давления, уровней электрической и магнитной составляющих электромагнитного поля в речевом диапазоне) в маломощные электрические сигналы, которые подаются на соответствующие входы сигнального концентратора (Рис.6.).

Рис.6. Сигнальный концентратор с микрофоном.

Сигнальный концентратор обеспечивает согласование датчиков с линейной частью прибора, усиление сигналов малых уровней, поступающих от датчиков, их преобразование в цифровую форму и передачу в управляющую ПЭВМ.

Сигнальный концентратор имеет три независимых канала, каждый из которых содержит прецизионные программно управляемые усилители, устройства электропитания датчиков и активные НЧ фильтры. Также в состав концентратора входит устройство управления, реализованное на базе микроконтроллера, устройство индикации, представляющее собой графический жидкокристаллический индикатор, 16-разрядный аналогово-цифровой преобразователь и устройство обмена информацией с ПЭВМ по последовательному интерфейсу.

Измерительные антенны, обеспечивающие измерение электрической и магнитной составляющих электромагнитного поля, а также устройства сопряжения с линией, обеспечивающие измерение уровней сигналов НЧ наводок в линиях ТСПИ, подключаются ко входу канала 1; вибродатчик (акселерометр), обеспечивающий измерение виброускорений, подключается ко входу канала 2; и микрофон, обеспечивающий измерение уровней звукового давления, подключается ко входу канала 3 концентратора.

Сигналы от датчиков, поступающие на входы многоканального сигнального концентратора, усиливаются управляемыми прецизионными усилителями соответствующих каналов и через НЧ фильтры подаются на входы многоканального АЦП концентратора. Устройство управления сигнального концентратора записывает измеряемые сигналы в цифровом виде в память, или передает их по последовательному порту через устройство обмена в управляющую ЭВМ, которая производит их дальнейшую обработку. Коэффициент усиления управляемых прецизионных усилителей задается программно с использованием соответствующих процедур СМПО комплекса. Также программно включается электропитание каналов и подключаемых к нему датчиков.

Сигнальный концентратор работает в централизованном и автономном режимах. В централизованном режиме он работает под управлением ПЭВМ, обрабатывающей результаты измерений в реальном масштабе времени. В автономном режиме он функционирует без подключения к ПЭВМ, записывает измеряемые сигналы в запоминающее устройство для их последующей обработки с использованием ПЭВМ. В автономном режиме управление концентратором производится с использованием клавиатуры, расположенной на передней панели.

Блок формирования тестовых акустических сигналов (Рис.7.) также функционирует как в централизованном, так и в автономном режиме.

Рис.7. Блок формирования тестовых акустических сигналов с акустической системой.

В централизованном режиме управление блоком осуществляется с использованием ПЭВМ, а в автономном - с использованием клавиатуры, расположенной на передней панели блока. Блок формирует шумовые, гармонические и речеподобные тестовые акустические сигналы различных уровней, требующиеся для реализации методик проверки выполнения норм по защите речевой информации. Для коррекции спектра тестовых сигналов блок имеет встроенный пятиполосный эквалайзер.

Подготовка к работе.

При полном развертывании комплекса необходимо выполнить следующую последовательность действий.

Присоединить сетевой шнур ко входу питания управляющей ПЭВМ и включить его в сеть, при этом сетевой тумблер «POWER» ЭВМ должен находится в положении “OFF” или “O”.

Открыть крышку-монитор управляющей ЭВМ.

Подключить выход концентратора «ПЭВМ (RS-232)» к последовательному порту управляющей ПЭВМ с помощью специального соединительного шнура («COM-COM DB» из комплекта концентратора), тумблер включения питания концентратора при этом должен находится в положении “O” (Выкл).

Подключить акустическую колонку к выходу «АКУСТ. СИСТЕМА» блока формирования тестовых акустических сигналов. Если есть необходимость работы блока под управлением ПЭВМ, то произвести его подключение к ПЭВМ.

В соответствии с задачами контроля произвести подключение измерительных датчиков к концентратору. При этом:

измерительный микрофон подключать ко входу 3-го канала концентратора;

вибродатчик подключать ко входу 2-го канала концентратора;

измерительные антенны или устройство сопряжения с линией подключать ко входу 1-го канала концентратора.

Размещение устройств, входящих в комплекс, внутри (снаружи) контролируемых объектов определяется в соответствии с требованиями методик проведения измерений при проверке выполнения норм по защите речевой информации.

Включение.

Для включения комплекса требуется выполнить следующую последовательность действий:

предварительно произвести развертывание комплекса;

сетевой тумблер «POWER» управляющей ЭВМ перевести в положение “ON” или “ I ”, при этом должна начаться «загрузка» операционной системы управляющей ЭВМ;

включить тумблер «ВКЛ» на передней панели концентратора, при этом на ЖКИ концентратора должно появиться рабочее меню;

включить тумблер «ВКЛ» на передней панели блока формирования тестовых сигналов, при этом на ЖКИ блока должно появиться рабочее меню;

после загрузки операционной системы ЭВМ «запустить» управляющую программу.

После выполнения данных действий комплекс готов к работе.

Проверка работоспособности.

Проверка работоспособности комплекса может быть выполнена после его развертывания и включения. Она состоит из последовательности трех проверок, включающих:

проверку работоспособности блока формирования тестовых акустических сигналов с усилителем мощности;

проверку работоспособности системы «управляющая ПЭВМ – концентратор»;

комплексную проверку работоспособности всей системы в целом.

При проверке работоспособности блока формирования тестовых акустических сигналов с усилителем мощности требуется выполнить следующие действия.

С использованием кнопок «Mode» и «►», «◄» выбрать вид сигнала «гармонический», нажать кнопку «Enter». С помощью кнопок «►», «◄» выбрать частоту акустического сигнала 1000 Гц. Нажать кнопку «Enter». С помощью кнопок «►», «◄» установить уровень тестового сигнала в пределах от 10 до 15 относительных единиц уровня. Нажать кнопку «Enter». После выполнения описанных операций акустическая колонка, подключенная к блоку формирования тестовых акустических сигналов должна начать излучение гармонического сигнала частотой 1 кГц. Его наличие свидетельствует о нормальном функционировании блока в режиме формирования тестового гармонического сигнала. Отключение сигнала произвести нажатием кнопки «Out» на панели управления блока.

С использованием кнопок «Mode» и «►», «◄» выбрать вид сигнала «Шум», нажать кнопку «Enter». Кнопками «►», «◄» установить уровень тестового сигнала в пределах 10-15 относительных единиц уровня и нажать кнопку «Enter». Блок формирования тестовых акустических сигналов должен начать излучение шумового сигнала, что является свидетельством его нормального функционирования в режиме формирования тестового шумового сигнала. Отключение сигнала произвести нажатием «Out» на панели управления блока.

При нормальном функционировании блока как в режиме формирования тестового гармонического, так и тестового шумового сигнала аппаратура формирования и излучения тестового сигнала считается работоспособной.

При проверке работоспособности системы «управляющая ЭВМ – концентратор» требуется выполнить следующие действия. Подключить к ПЭВМ сигнальный концентратор. Произвести загрузку управляющей программы. После загрузки экранной формы приветствия произвести автоматическое подключение сигнального концентратора. Для этого следует на экранной форме приветствия нажать с помощью манипулятора ПЭВМ кнопку «Работа с прибором в дистанционном режиме». Если при этом происходит загрузка основной экранной формы СМПО, то это означает, что произошло автоматическое подключение концентратора к ПЭВМ и является свидетельством работоспособности концентратора и СМПО управляющей ПЭВМ.

При проведении комплексной проверки работоспособности всей системы в целом требуется выполнить следующую последовательность действий.

Разместить предварительно подключенный к сигнальному концентратору измерительный микрофон на расстоянии 1-3 м от блока тестовых акустических сигналов. Перевести блок формирования тестовых сигналов в режим излучения тестового гармонического сигнала.

Выбрать вид контроля на главной экранной форме СМПО в режиме централизованного управления концентратором - «Акустический контроль». Нажатием кнопки «Тест» и выбором коэффициента усиления добиться изображения сигнала, при котором его осциллограмма близка к форме гармонического сигнала (отсутствуют видимые искажения). Наличие такой осциллограммы на экране монитора ПЭВМ свидетельствует о полной работоспособности всей контрольно-измерительной системы.

Если результаты одного из перечисленных тестов являются неудовлетворительными, то необходимо выявить причины неисправности и устранить ее, используя при этом технические описания и инструкции по эксплуатации к блоку формирования тестовых сигналов и концентратору.

Порядок работы с комплексом.

Общие сведения.

Проверка выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу заключается в количественной оценке величины показателя эффективности защиты речевой информации с последующим ее сравнении с нормированными значениями.

Эффективность защиты речевой информации от утечки по акустическому каналу оценивается по одному из двух показателей:

- словесная разборчивость речи W, определяемая в контрольных точках;
- распределение отношений «речевой сигнал/акустический шум» E_i, в октавных полосах частот в контрольных точках.

Проведение проверки выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу производится в 5 этапов:

1. подготовительный этап;
2. этап выбора контрольных точек;
3. этап размещения аппаратуры формирования тестовых акустических сигналов с акустической системой;
4. этап проведения измерений и расчетов;
5. этап подготовки протокола измерений.

Подготовительный этап.

На подготовительном этапе необходимо произвести предварительную оценку звукоизоляции помещений с целью определения наиболее вероятных разведопасных направлений. Уточнить положение ограждающих конструкций помещения и элементов технических систем относительно установленной границы контролируемой зоны. Уточнить категорию объекта контроля, а также условия речевой деятельности в контролируемом помещении.

Этап выбора контрольных точек.

На данном этапе необходимо произвести выбор контрольных точек.

Контрольными точками являются места возможной установки акустических датчиков аппаратуры акустической речевой разведки, или места непреднамеренного прослушивания речи, в которых производится измерение отношений «сигнал/шум». При выборе контрольных точек необходимо строго следовать рекомендациям, изложенным в нормативно-методических документах по контролю эффективности защиты информации от акустической речевой разведки. Возможные варианты утечки речевой информации из помещения представлены на рис.8.

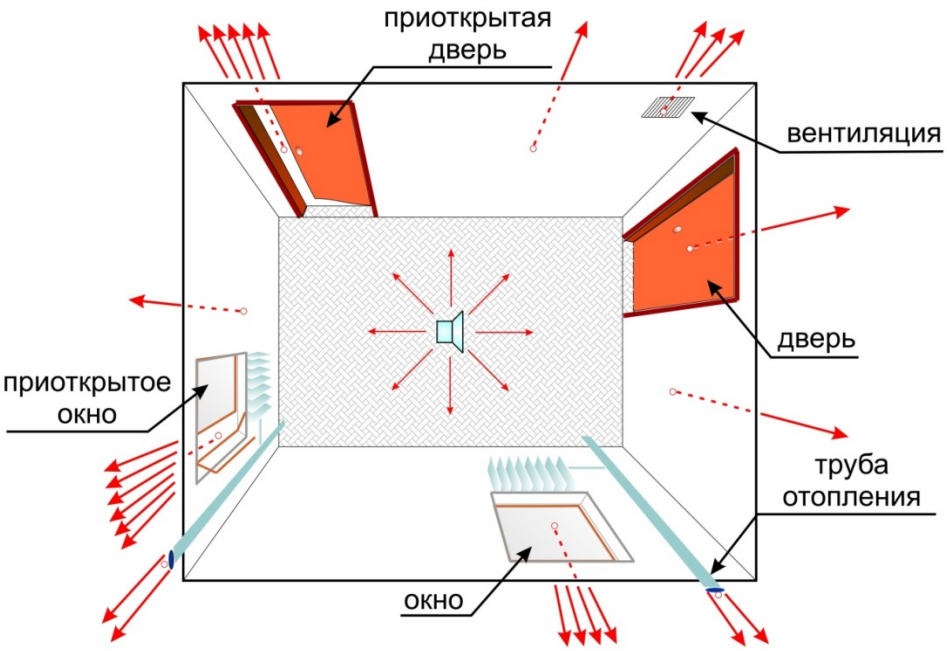


Рис.8. Утечка речевой информации из помещения.

Этап размещения аппаратуры формирования тестовых акустических сигналов с акустической системой.

Разместить аппаратуру формирования тестовых акустических сигналов в контролируемом помещении исходя из особенностей речевой деятельности в этом помещении:

1. Если источник речи локализован в помещении в пределах конкретного рабочего места, то акустическую систему установить непосредственно на рабочем месте и ориентировать ее рабочую ось в направлении контрольной точки по нормали к плоскости ограждающей конструкции.
2. Если в пределах рабочего помещения место источника речи не зафиксировано, то акустическую систему разместить на высоте 1,5 м от пола на расстоянии 1 м от вертикальной поверхности ограждающей конструкции. Рабочую ось излучения акустической системы сориентировать по нормали к обследуемой ограждающей конструкции. Аналогичные расстояния и направления излучения соблюдать при обследовании элементов инженерно-технических систем.
3. Если обследуемой конструкцией является пол или потолок, то акустическую систему установить в центре помещения на высоте 1,5 м от пола и направление его излучения сориентировать по нормали к полу (потолку).
4. При контроле помещений, оборудованных системами звукоусиления, акустическую систему разместить перед микрофоном (микрофонами) системы звукоусиления. Установить уровень сигнала согласно действующим нормам.

Этап проведения измерений и расчетов.

На этапе измерения отношений «речевой сигнал/акустический шум» последовательно произвести следующие измерения:

1. измерить уровень тестового акустического сигнала, формируемого акустической системой внутри контролируемого помещения (при установке уровня следует руководствоваться действующими нормативными документами);

2. измерить уровень фоновых акустических шумов и уровня тестового акустического сигнала в каждой из выбранных контрольных точек;

3. рассчитать показатели защищенности информации от акустической разведки с помощью специального математического программного обеспечения (СМПО) комплекса.

Рассмотрим подробно порядок проведения измерений:

При измерении уровня тестового акустического сигнала внутри контролируемого помещения в случае отсутствия в нем средств звукоусиления (СЗУ) используем блок формирования тестовых акустических сигналов «СПРУТ-Г3».

Для подготовки его к работе необходимо выполнить следующую последовательность действий:

1. Достать прибор из упаковки;

2. Подключить акустическую систему к линейному выходу прибора (АС);

3. Включить тумблер включения питания прибора «ВКЛ»;

4. После выполнения всех пунктов на ЖКИ прибора «высвечивается» серийный номер прибора, после чего он переходит в режим выбора вида тестового сигнала.

В качестве тестового акустического сигнала необходимо использовать «белый шум», применяя необходимый для корректного измерения уровень сигнала.

Включение тестового акустического сигнала на излучение следует производить непосредственно перед началом проведения измерений.

Далее необходимо развернуть и включить сигнальный концентратор «СПРУТ-М3».

Для этого необходимо выполнить следующую последовательность действий:

1. Достать прибор из упаковки.

2. Подключить к входу 3 канала измерительный микрофон используя соответствующий шнур адаптера. Измерительный микрофон разместить на расстоянии 1 м от колонки блока формирования тестовых акустических сигналов.

3. Подключить сигнальный концентратор к порту управляющей ПЭВМ.

4. Включить тумблер включения питания прибора «ВКЛ», на ЖКИ прибора появится серийный номер прибора, после чего он переходит в режим выбора типа канала (используемого датчика).

5. Нажать кнопку «Mode», используя клавиши «▲ ▼» в предложенном списке режимов выбрать «режим управления по USB» и активировать его клавишей «Enter».

После выполнения данных действий концентратор полностью готов к работе.

Запуск и выбор режима работы специального математического программного обеспечение (СМПО).

Специальное математическое программное обеспечение (СМПО) предназначено для управления аппаратурой комплекса «Спрут-мини», получения данных от датчиков, обработки полученных результатов и формирования отчетов установленной формы по результатам проведенных измерений.

Работа с СМПО комплекса «Спрут-мини» производится после развертывания и включения средств, входящих в состав комплекса. Запуск СМПО производится с помощью исполняемого файла, который может быть выбран через меню «Пуск», «Программы» ОС «Windows» либо через «Проводник».

При запуске СМПО на экране управляющей ПЭВМ отображается главная экранная форма и устанавливается вид контроля «Акустический контроль» Пользователь задает режим работы самостоятельно, пользуясь органами управления главной экранной формы.

Проведение измерений акустического контроля включает следующую последовательность основных операций.

Выбор режима централизованного управления концентратором.

После выполнения предыдущих пунктов и перехода концентратора в централизованный режим (режим управления по USB) в главной экранной форме автоматически активизируются кнопки старта измерения, кнопка загрузки результатов единичных измерений (банков памяти) концентратора, кнопка выбора коэффициентов усиления каналов и появится индикатор уровня заряда батареи.

Выбор вида контроля производится в главной экранной форме кнопкой «Вид контроля», нажатие которой разворачивает меню с пунктами «Акустический контроль», «Виброакустический контроль» и «Контроль наводок в линиях ТСПИ». При загрузке главной экранной формы вид «Акустический контроль» устанавливается по умолчанию.

При выборе вида контроля «акустический контроль» активизируется кнопка выставления коэффициента усиления 3 канала концентратора.

Выбор категории контролируемого объекта. В любом из выбранных видов контроля перед началом проведения измерений необходимо правильно выбрать категорию контролируемого объекта. Для этого необходимо нажать кнопку выбора категории контролируемого объекта и в открывшемся списке установить номер категории объекта.

Выбор требуемого значения коэффициента усиления концентратора. Производится путем нажатия кнопки «Тест» и визуальной оценкой осциллограммы измеряемого (контролируемого) сигнала. Правильность выбранного коэффициента усиления (кнопка «КУ» на главной экранной форме) подтвер-

ждается формой осциллограммы, которая не содержит явных признаков искажений сигнала («обрезание» сигнала в максимумах амплитуды) и свидетельствует об устойчивом приеме сигнала (сигнал различим на экранной форме). Подбор коэффициента усиления производится при отрицательных результатах тестирования.

Тестирование контролируемых сигналов производится перед проведением измерений и преследует цель удостоверится, что на входе выбранного канала присутствует сигнал и что коэффициент усиления выбранного канала установлен правильно: усилитель не входит в режим «насыщения», уровень сигнала на его выходе не слишком мал для проведения измерений (рекомендуемые значения амплитуд контролируемых сигналов (-1,8…+1,8) В.

Тестирование контролируемых сигналов производится нажатием кнопки «Тест», после чего появляется временная развертка измеряемого сигнала. Если сигнал на временной развертке не удовлетворяет требованиям, приведенным выше, необходимо изменить значения коэффициента усиления используемого канала концентратора и повторить тестирование.

Проведение цикла измерений при подсоединенном сигнальном концентраторе «СПРУТ-М3» осуществляется нажатием кнопки «СИГНАЛ», «ШУМ» или «С+Ш»

Нажатием на кнопку «СИГНАЛ» (кнопка старта измерения информативного сигнала) осуществляется измерение и загрузка данных сигнала из сигнального концентратора «СПРУТ-М3». При этом на экране спектрограмм контролируемых сигналов отображается спектр зеленого цвета рис.9.

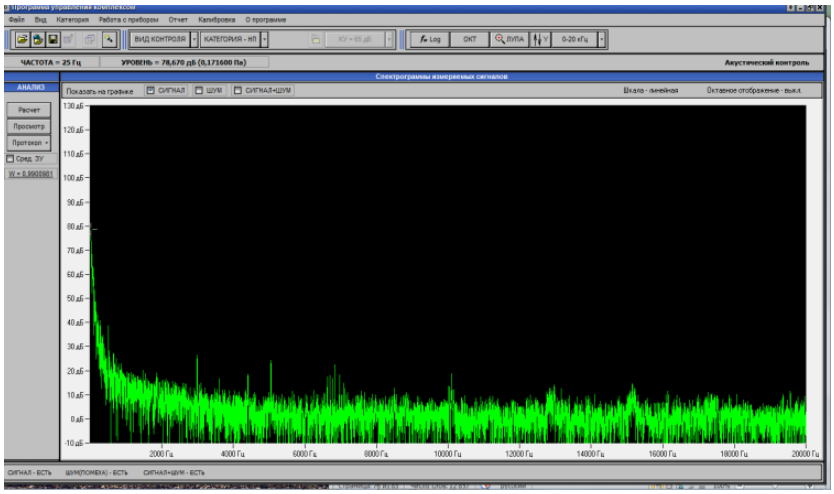


Рис.9. Измерения информативного сигнала

Нажатием на кнопку «ШУМ» (кнопка старта измерения фонового сигнала) осуществляется измерение и загрузка данных фона. При этом на экране спектрограмм контролируемых сигналов отображается спектр голубого цвета рис.10.

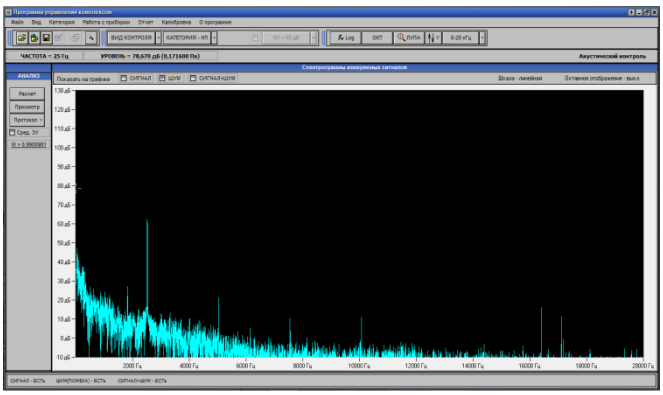


Рис.10. Измерения фонового сигнала (шума).

Нажатием на кнопку «С+Ш» (кнопка старта измерения суммарного информативного сигнала и фонового шума) осуществляется измерение и загрузка данных суммарного информативного и фонового сигнала из сигнального концентратора «СПРУТ-М3». При этом на экране спектрограмм контролируемых сигналов отображается спектр красного цвета рис.11.

После проведения цикла измерений и расчета активизируются кнопки просмотра результатов контроля. При нажатии на кнопку выхода в режим просмотра результатов контроля или «Просмотр результатов контроля» главного меню «Отчет» осуществляется переход к экранной форме просмотра результатов контроля для видов контроля «Акустический контроль»

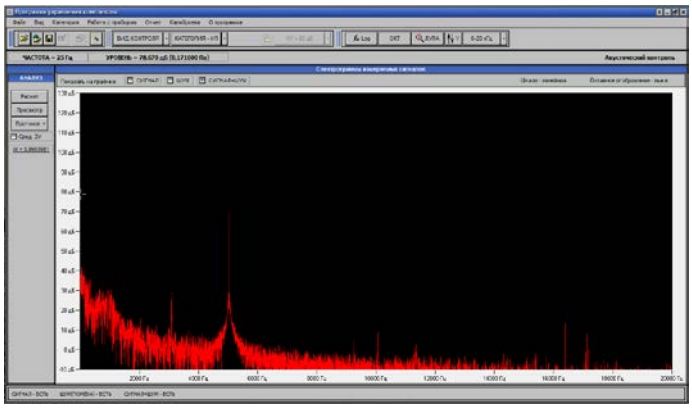


Рис.11. Измерения суммарного информативного сигнала и фонового шума

Оценка эффективности защиты информации производится нажатием кнопки «Расчет» (кнопка активна, если проведена тройка измерений «Сигнал», «Шум» и «С+Ш»), в результате чего в левой нижней части главной экранной формы появляется значение показателя «Словесная разборчивости речи» (W). Кнопка «Просмотр» инициализирует экранную форму, отображающую результаты оценок промежуточных показателей, отображаемых в отчетных документах.

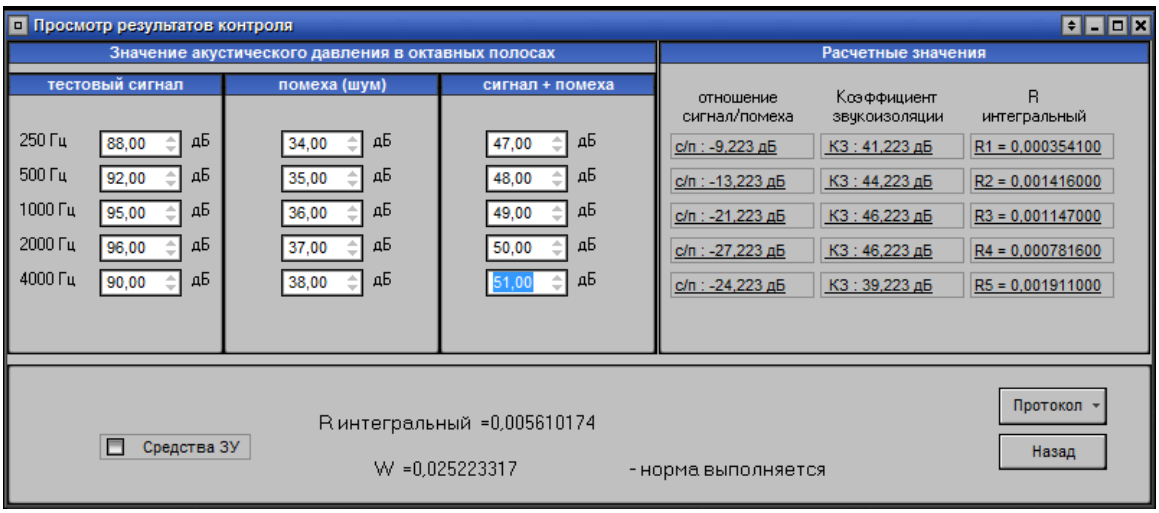


Рис.12. Экранная форма просмотра результатов для акустический контроля.

Этап подготовки протокола измерений.

Оформление отчетных документов является неотъемлемой частью проведения контроля и осуществляется по формам, установленным действующими нормативными документами. Они включают в себя данные измерений и расчетов для контрольных точек, в которых проводились измерения. Для составления протоколов следует из главной экранной формы запустить процедуру «Протокол» и «Новый протокол». Программа сгенерирует протокол измерений для данной контрольной точки. В протоколе необходимо указать недостающие сведения в соответствии с указанными пунктами

Проверка выполнения норм эффективности защиты речевой информации от утечки по виброакустическому каналу при использовании комплекса «Спрут-мини А» выполняется по контрольным точкам. Контрольными точками являются места возможной установки вибрационных датчиков аппаратуры акустической речевой разведки - коммуникации, выходящие за границу контролируемой зоны, ограждающие конструкции, или места расположения отражающих поверхностей, уязвимых для лазерного съема речевой информации (в первую очередь это оконные стекла).

В меню выбора вида контроля выбирается режим «Виброакустический контроль». В качестве приемного датчика при измерениях используют вибродатчик (акселерометр).

Программно-аппаратный комплекс «Навигатор» (в состав которого входит программное обеспечение «Навигатор») предназначен для проведения:

1. специальных исследований;
2. аттестационных испытаний;
3. контроля защищенности объектов автоматизации от утечки информации через побочные электромагнитные излучения и наводки (ПЭМИН) и электроакустические преобразования, распространяющиеся как в радиоэфире, так и в проводных линиях, в соответствии с действующими нормативно-методическими документами.

А так же для поиска, измерения характеристик ПЭМИН при проведении инженерных исследований различной аппаратуры.

Программа «Навигатор» предназначена для создания на ее основе программно-аппаратного комплекса. Она разработана в соответствии с требованиями «Сборника методических документов по контролю защищенности информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)», введенного в действие приказом ФСТЭК России от 30.12.2005 года.

Данный комплекс предназначен для избавления оператора от выполнения однообразных действий при исследованиях и измерениях ПЭМИН. Он также увеличивает достоверность измерений и способствует значительному уменьшению времени на оформление отчетной документации.

Состав комплекса.

Состав комплекса «Навигатор - П5Г» представлен оборудованием и программным обеспечением.

Основное оборудование:

– анализатор спектра (измерительный приемник);

– комплект антенн, работающих в диапазоне частот анализатора спектра (измерительного приемника);

– пробник напряжения;

– специальное программное обеспечение «Навигатор»;

– Notebook для управления анализатором спектра (измерительным приемником) и производства расчетов.

Вспомогательное оборудование:

– эквивалент сети;

– токосъемник;

– стол поворотный диэлектрический;

– штатив диэлектрический.

В состав программного комплекса «Навигатор» входят поисковая и измерительная программа «Навигатор» и программа расчета требуемых показателей защищенности «Навигатор-С». Поисковая и измерительная программа осуществляет поиск и измерение пиковой амплитуды сигналов ПЭМИН и уровня шума. Расчетная программа производит расчет требуемых показателей защищенности.

В программном обеспечении «Навигатор» реализован математический аппарат, позволяющий корректно измерять шум, генерируемый САЗ, с использованием детекторов, отличных от среднеквадратичного. Работа данных алгоритмов основывается на аналитических зависимостях между разными типами детекторов, приведенных в международных нормативных документах в области метрологии (рис. 13).

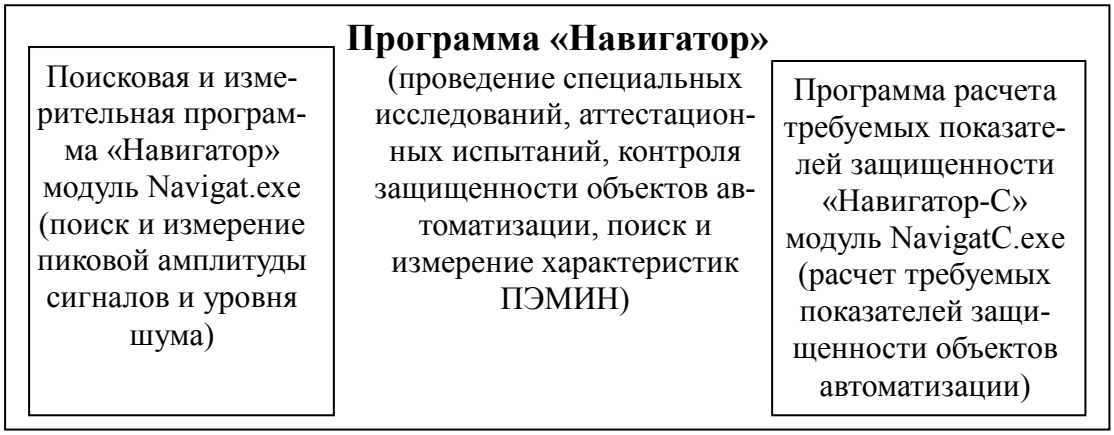


Рис. 13. Схема состава и назначения программы «Навигатор»

Основные технические данные и характеристики.

Характеристика	Значение
Диапазон рабочих частот: – определяется ТХ измерительного оборудования; программа ограничений на диапазон не имеет – по электрической составляющей электромагнитного поля – по магнитной составляющей электромагнитного поля – при измерении наводок	 9 кГц…1800 МГц от 0,1 кГц до 13,2 ГГц от 0,03 кГц до 30 МГц от 0,03 кГц до 100 МГц
Устанавливаемые полосы пропускания не менее	0,01; 0,03; 0,1; 0,3; 1; 3; 10; 30; 100; 300 кГц
Предел основной абсолютной погрешности измерения частоты ПЭМИН	Не хуже ± одна установленная полоса пропускания
Динамический диапазон измерения уровней ПЭМИН	Не менее 82 дБ
Уровень собственных шумов	Не хуже 0 дБмкВ, при полосе пропускания 1 кГц на частоте 100 МГц
Предел основной относительной погрешности измерения уровня ПЭМИН: – в диапазоне частот 0,1 и выше – в диапазоне частот 0,03…0,1 кГц	 ±2 дБ ±3 дБ
Тип детектора	Пиковый
Масса нетто (при использовании в качестве управляющей подсистемы ПЭВМ типа Notebook)	от 15,5 до 30 кг
Электрическое питание: – напряжение – частоты	 220 ($_{-15\%}^{+10\%}$) В 50 ± 1 Гц
Потребляемая мощность (при использовании в качестве управляющей подсистемы ПЭВМ типа Notebook)	от 110 до 350 Вт
Рабочие условия эксплуатации: – температура окружающего воздуха – относительная влажность воздуха (при температуре 25ºС)	 от 10 до 35 ºС до 80 %
Точность определения частоты ПЭМИН, типовая	± одна/две установлен-

	ные полосы пропускания
Диапазон измеряемых уровней ПЭМИН, типовой	0…100 дБмкВ/м
Точность измерения уровня ПЭМИН, типовая	±2 дБ + точность калибровки антенны
Тип исследований	1. специальное исследование технического средства; 2. контроль защищенности объектов автоматизации; 3. поиск сигналов электроакустических преобразователей; 4. инженерные исследования технических средств на предмет ПЭМИН.
Рассчитываемые показатели защищенности	R2, R1, R1´; отношение сигнал/шум на границе контролируемой зоны; требуемая защищенность цепей электропитания и заземления.

Методы поиска сигналов ПЭМИН, реализуемые в программе «Навигатор».

В программно-аппаратном комплексе используется 4 метода поиска ПЭМИН:

- метод сравнения панорам;
- аудио-визуальный метод;
- экспертный метод;
- параметрически-корреляционный метод.

Данные методы различаются по степени принятия участия в них человека (опертора). Полностью автоматический метод – *параметрически-корреляционный*. Далее, учитывая уровень автоматизации, можно обозначить *разности панорам*. *Аудио-визуальный метод* и *метод поиска по гармоникам следует* считать автоматизированными методами.

По полноте и достаточности результатов методы поиска можно разместить в обратном порядке по степени автоматизации (потому что зачастую исследуют слабые сигналы, корректно идентифицировать которые возможно лишь оператору, обладающему достаточным опытом и профессиональной интуицией). Наилучшие показатели показывает *экспертный метод*. Затем *аудио-визуальный метод*, и замыкает ряд *метод разности панорам*.

Метод разности панорам.

Основополагающий принцип поиска сигналов ПЭМИН в этом методе основан на том, что тестовый сигнал создает периодическую последовательность сигналов в электрических цепях, которые в свою очередь обуславливают появление откликов в радиоэфире. Созданные сигналы в радиоэфире обладают постоянными характеристиками по амплитуде и частоте. Стабильность частоты данных сигналов зависит только от стабильности опорного генератора (кварца), а нестабильность амплитуды сигналов зависит от нестабильности амплитуды источника сигнала в и отношения сигнал/шум сигнала в радиоэфире. Влияние шума на сигнал проявляется при отношении сигнал/шум ниже 10дБ: результирующий сигнал в радиоэфире суммируется с шумом по формуле

$$E_{результирующее} = \sqrt{E^2_{\text{сигнала}} + E^2_{шума}}, \text{ (мкВ)}$$

Если сигнал выше шума более чем на 10дБ (более чем в три раза), то шум оказывает влияние на амплитуду сигнала самой незначительной степени. Иначе, шум модулирует результирующий сигнал. Снижение влияния шума на сигнал достигается алгоритмами усреднения.

Для поиска сигналов выполняют пару измерений уровней магнитного и электрического полей рассматриваемого объекта – первый раз измерения проводят при отсутствующем тестовом сигнале, второй раз при включенном тестовом сигнале. Затем график уровней электромагнитного поля, полученный в отсутствие тестового сигнала, вычитают из графика уровней электромагнитного поля при включенном тестовом сигнале. Зафиксированные точки на определенных частотах, в которых сигналы из второго графика превысили сигналы из первого графика на некоторый порог, записывают в перечень частот вероятных сигналов ПЭМИН.

Кроме истинных частот ПЭМИН (возникших сигналов) в список найденных сигналов

попадают и ложные частоты – шумы и излучения других радиотехнических средств, включившихся в работу между двумя измерениями. Поэтому, все значения сигнала, зафиксированные в списке, следует исследовать на принадлежность к ПЭМИН проверяемой аппаратуры. Для этого в программе используется 2 режима, реализующие операцию автоматической верификации.

Обе верификации можно проводить по несколько раз. Чем больше циклов верификаций, тем больше отбраковывается ложных сигналов.

Окончательное решение по поводу принадлежности точек списка к ПЭМИН принимает

оператор в экспертном режиме работы на этапе измерения амплитуды сигналов ПЭМИН.

Аудио-визуальный метод поиска.

Этот метод считается довольно простым, так как в нем осуществляется визуальный контроль электромагнитного спектра. Данный метод широко распространен на практике, так как предельно прост и понятен.

На первом этапе данного метода происходит получение двух спектров электромагнитной обстановки – с выключенным и включенным тестовым сигналом.

Далее оператор визуально оценивает измеренные графические изображения и анализирует подозрительные сигналы. Вся работа производится только с помощью мышки. Для работы предоставлены широкие возможности: масштабирование графиков по осям, подкраска подозрительных сигналов, отображение осциллограмм и спектров подозрительных сигналов, виртуальная панель управления измерительным прибором и т.д.

После нахождения информативных сигналов, занесение их в список (частота, уровень сигнала и шума, полоса пропускания, тип поля) осуществляется в "экспертном" режиме работы.

Метод позволяет автоматизировать несколько трудоемких операций, которые встречаются при ручных измерений: поиск сигналов, поиск максимума сигналов и отсеивание неинформативных боковых лепестков вызванных энергией более низкочастотных модулирующих сигналов. Для визуального обнаружения слабых сигналов рекомендуется использовать метод усреднения при измерении панорам электромагнитной обстановки с включенным и выключенным тестом.

Метод поиска по гармоникам.

Рассматриваемый метод является вариантом известного метода поиска сигналов на частотах их гармоник. Любая периодическая последовательность цифровых сигналов образует в радиоэфире ряд гармоник. Все сигналы при этом кратны $1/t_и$ и $1/T$, где $t_и$ – длительность импульса тестового сигнала, T – период следования тестового сигнала. Данный метод широко используется при ручных исследованиях, однако занимает много времени в силу того, что оператор не знает точную частоту сигнала первой гармоники. По этой причине поиск производят в окрестностях рассматриваемой частоты, что влечет за собой затраты временных ресурсов.

Метод компенсирует указанный недостаток следующим образом: максимально точно измеряется частота первой гармоники и затем, прогнозируется частота следующей. После установки на определенную частоту происходит поиск максимума сигнала, и производится уточнение значения частоты первой гармоники по частоте найденного сигнала. Панорамы электромагнитного состояния поля измеряются при использовании широких полос пропускания (10-100 кГц, на что расходуется 30-40 секунд). Находится любой информативный сигнал ПЭМИН и по нему максимально точно определяется частота первой гармоники. Далее производится сканирование частот всех гармоник с более узкой полосой пропускания с периодической подстройкой частоты первой гармоники по уточненной частоте более высших гармоник. Данный метод позволяет использовать максимальную чувствительность измерительного прибора и очень точно настраиваться на прогнозируемую частоту следующей гармоники.

Необходимо отметить, что исследование сигналов на частотах гармоник хотя и является практикой работы, но недостаточно для полноценного исследования технического средства, так как не учитывает возможность наличия сигналов на частотах не кратных частоте первой гармоники (например, сигналов паразитной генерации). Для поиска таких сигналов необходимо использовать любой из предыдущих методов.

Параметрически-корреляционный метод исследования мониторов.

Данный метод автоматически проверяет принадлежность сигналов из списка предварительно найденных сигналов (с помощью методом разности

панорам) при включенном и выключенном тестовом сигнале к ПЭМИН монитора.

Начало работы данного режима аналогично началу работы метода разности панорам. Но вместо верификаций списка сигналов по параметру "энергетики", все частоты сформированного списка подозрительных сигналов проверяются по параметрическому критерию. Для каждого сигнала строится его параметрический портрет, который сравнивается с параметрическим портретом сигнала монитора. После анализа всех сигналов списка параметрические портреты сравниваются между собой, отбрасываются ложные сигналы и сигналы боковых частот модуляционной составляющей строчной развертки.

Далее прогнозируется частота первой гармоники и выполняется поиск ряда частот гармоник, аналогично методу поиска по гармоникам, но в автоматическом режиме. Каждый сигнал анализируется при нескольких полосах пропускания и для расчета параметров выбирается та полоса пропускания, при которой наиболее качественно определяются параметры сигнала. При поиске гармоник, по каждому следующему найденному сигналу гармоники уточняется частота первой гармоники.

Другой вариант использования данного метода заключается в том, что указывается частота найденного другими методами сигнала ПЭМИН по которому строится параметрический портрет. Далее по этому портрету производится поиск остальных сигналов ПЭМИН, включая сигналы гармоник.

Этот метод следует использовать только для более углубленного поиска сигналов гармоник ряда найденных другими методами сигналов.

Сходства и различия описанных ранее методов для удобства представлены в таблице.

Название метода	Требования к участию оператора	Эффективность метода	Время поиска (для типового ТС "монитор ПЭВМ")
Разности панорам	необходимо только для включения и выключения тестового режима работы и контроля принятых программой решений на этапе измерения амплитуды сигналов ПЭМИН	Хорошо определяются мощные сигналы ПЭМИН, у которых отношение сигнал/шум превышает 6-10дБ	5-10 минут
Аудио-визуальный	во всех этапах работ	обнаруживает практически все сигналы с положительным отношением сигнал/шум для выбранной полосы пропускания	3-10 минут
Поиска по гармоникам	во всех этапах работ	обнаруживает все сигналы ПЭМИН с предельно достижимой чувствительностью измерительного прибора, самая высокая эффек-	8-15минут

		тивность из всех методов	
Параметрическо-корреляционный	необходимо только для включения и выключения тестового режима работы исследуемого ТС	в случае, если исследуемое ТС выполнено в защищенном исполнении или имеет слабые ПЭМИН или при поиске антенна неправильно расположена относительно ТС, имеется вероятность того, что метод не найдет сигналов ПЭМИН или найдет ложные сигналы ПЭМИН.	20-40 минут

Режимы работы в поисковой и измерительной программе "Навигатор".

Для проведения работ по поиску сигналов ПЭМИН, измерению их амплитуды и проведения расчетов необходимых показателей защищенности программа включает в себя 8 режимов работы:

– "Настройка: оборудование, антенны, частотные диапазоны";
– "Измерение индустриального шума";
– "Обнаружение ПЭМИН";
– "Автоматическая верификация результатов 1" (используются только в методе разности панорам);
– "Автоматическая верификация результатов 2" (используются только в методе разности панорам);
– "Экспертный режим";
– "Измерение шума САЗ";
– "Обработка данных и создание отчета".

В поисковой и измерительной программе "Navigat.exe" реализовано 7 режимов: "Настройка: оборудование, антенны, частотные диапазоны", "Измерение индустриального шума", "Обнаружение ПЭМИН", "Автоматическая верификация результатов 1", "Автоматическая верификация результатов 2", "Измерение шума САЗ" и "Экспертный режим".

Режим "Обработка данных и создание отчета" реализован в расчетной программе "NavigatC.exe".

"Настройка: оборудование, антенны, частотные диапазоны" используется для выбора измерительного оборудования, занесения калибровочных данных используемых антенн и формирования задания на поиск сигналов ПЭМИН.

"Измерение индустриального шума" и "Обнаружение ПЭМИН" используются для измерения спектра электромагнитной обстановки с выключенным и включенным тестовым сигналом для всех методов поиска, а так же для формирования списка вероятных частот ПЭМИН при использовании метода разности панорам.

"Автоматическая верификация результатов 1" и "Автоматическая верификация результатов 2" используются для отсеивания ложных сигналов при использовании метода разности панорам.

"Экспертный режим" используется для формирования списка сигналов ПЭМИН и для проверки и ручной коррекции списка найденных частот и для измерения амплитуды сигналов ПЭМИН с учетом вектора поляризации и диаграммы направленности.

"Измерение уровня САЗ " предназначен для измерения уровня САЗ и ЛСАЗ, сохранения этих данных и использование их в расчетной программе.

"Обработка данных и создание отчета" предназначен для обработки ранее собранных данных с целью расчета требуемых показателей защищенности. При вызове данного режима запускается расчетная программа "NavigatC.exe" а собранные данные по обнаруженным частотам ПЭМИН автоматически передаются и отображаются в расчетной программе.

Для каждого режима работы существуют свои собственные окна отображения информации и элементы управления. Вместе с тем, имеются органы управления, существующие во всех режимах.

Исследованию ПЭМИН подлежат различные элементы ПЭВМ (видеоподсистема, накопители на жестком и гибком дисках, устройства CD и DVD, устройства внешней флеш-памяти, клавиатура, принтеры и др.). Однако практический опыт показал, что наибольшее излучение формирует монитор. Соответственно, обнаружив ПЭМИН монитора и выполнив мероприятия по защите информации от утечки по данному каналу, можно с достаточной вероятностью гарантировать защиту от утечки по каналу ПЭМИН других элементов и устройств.

Рассмотрим пример выполнения таких задач, как:

– специальные исследования,
– аттестационные испытания,
– контроль защищенности ОИ от утечки информации за счет ПЭМИН.

Для решения данных задач последовательность действий на начальном этапе будет одинаковой.

Условно назовем первый блок действий «Поисковым этапом».

Здесь требуется обнаружить все радиоизлучения в указанном диапазоне частот. Как было описано ранее, в ПАК «Навигатор» существует 4 метода поиска ПЭМИН, однако на практике удобнее пользоваться не одним определенным методом, а комбинировать их в «Экспертном режиме» работы, для получения наиболее точного результата исследования.

Одной из главных целей для оператора в таком «Комбинационном методе» является обнаружение первой гармоники тест-сигнала. Для этого оператору необходимо осуществить поиск частоты, начиная с нижнего порога заданного диапазона, при которой в осциллографическом режиме работы анализатора появится изображение тест-сигнала явно выраженной формы меандра (Рис.14.).

При точном значении частоты первой гармоники (частота электрической составляющей для монитора обычно располагается в районе 30 МГц), программа автоматически найдет частоты других гармоник (кратных и, как показывает опыт, нечетных), на которых так же имеются излучения тест-сигнала.

Рис.14. Тест-сигнал формы меандра.

Сформированный по показаниям анализатора перечень сигналов подлежит корректировке путем анализа на принадлежность имеющихся сигналов к излучениям, относящимся именно к проверяемому техническому средству, так как значительная часть из обнаруженных приемным устройством сигналов может оказаться внеполосными излучениями промышленного, бытового или иного оборудования.

На втором этапе (условное название «Исследование ПЭМИН») работа оператора заключается в измерении ПЭМИН на корректном (определенном нормативно-методической документацией) расстоянии и уточнении значений характеристик радиоизлучений.

Дальнейшие действия определяются целью проводимых работ.

Выполняя специальные исследования необходимо определить возможные технические каналы утечки защищаемой информации. Грубо говоря, следует подтвердить факт наличия ПЭМИН исследуемой аппаратуры. Используя программу «Навигатор», оператору потребуется составить список сигналов с указанием уровня излучения, амплитуды сигнала и шума и значения частоты. Эти действия выполняются на описанных выше этапах (Поисковый этап, Исследование ПЭМИН).

При проведении аттестационных испытаний требуется исследовать не только ПЭМИН, но и определить эффективность работы средства защиты. Необходимо исследовать электромагнитную обстановку, формируемую системой активного зашумления (САЗ), например, генератором шума. С использованием ПАК «Навигатор» будут производиться измерения электромагнитных сигналов в отсутствии излучения генератора, а затем – с работающим генератором шума. В итоговых расчетах будет констатироваться выполнение/невыполнение нормы защиты.

Организация контроля защищенности потребует аналогичных действий, которыми сопровождаются аттестационные испытания.

Упрощенно алгоритм мероприятий можно представить в виде схемы на рисунке 15.

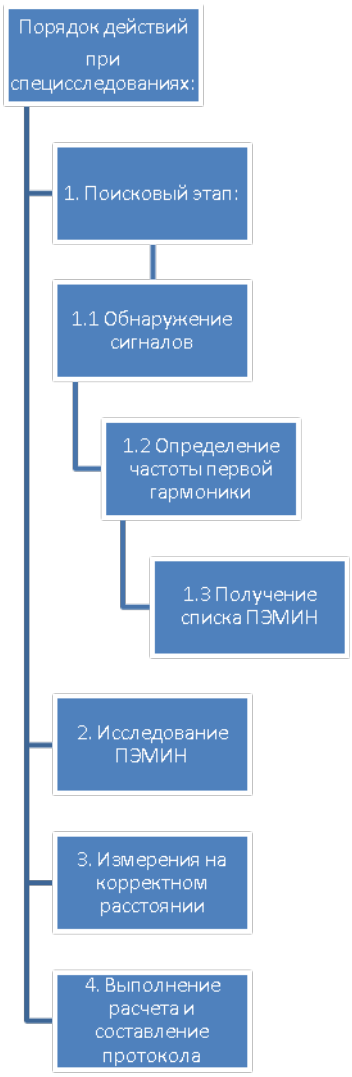


Рис. 15. Алгоритм мероприятий при проведении специсследования.

Выполнение задания «Проведение специального исследования монитора».

1. Подключить аппаратуру к источнику эталонного электропитания.

Соединить соответствующие разъемы кабелей, идущих от:

– исследуемого ТС;
– анализатора спектра;
– ноутбука с расчетной программой;
– поворотного стола;
– блока питания развязывающего устройства антенны;

в гнезда на задней стенке источника эталонного электропитания (Рис.16).

Рис.16. Источник эталонного электропитания.

2. Соединить ноутбук HP Pavilion и анализатор спектра E 4405B ESA-E с помощью интерфейсного кабеля GPIB-PCMCIA, подсоединяемого к специальной плате NI ExpressCard-GPIB, вставляемой в корпус ноутбука (Рис.17).


Рис.17. Соединение ноутбук и анализатор спектра.

3. Подготовить измерительные антенны к работе.

3.1.Закрепить антенну на штативе, соединить ее с развязывающим устройством и анализатором спектра.

3.2. Сориентировать антенну напротив диэлектрического стола таким образом, чтобы ее диаграмма направленности располагалась корректно для выполнения достоверных измерений. Антенны расположить так, как показано на рисунках 18 и 19.

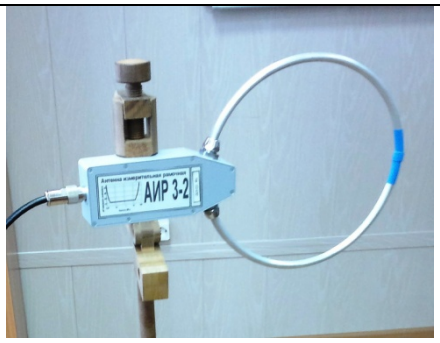


Рис.18. АИР 3-2	Рис. 19. АИ 5-0

Плоскость, образуемая рамкой должна располагаться перпендикулярно к исследуемому ТС. Такая ориентация антенн не является единственно правильной. В дальнейшем, при исследовании ТС на корректном расстоянии, антенны нужно будет вращать для того, чтобы добиться максимального показания уровня сигнала ПЭМИН.

4. Подключить источник эталонного электропитания в сеть общего пользования и включить его.

Тумблер ВКЛ/ВЫКЛ перевести вверх, нажать и удерживать 3 секунды кнопку ВКЛ/ВЫКЛ, дождаться появления желтого индикатора под надписью ВНИМАНИЕ, нажать и удерживать до появления звукового сигала кнопку ВЫБОР.

Правильная работа источника – зеленое свечение индикатора над надписью НОРМА.

5. Подготовить исследуемое техническое средство к запуску тестового режима работы.

5.1. Установить исследуемое ТС на диэлектрический поворотный стол.

5.2. Произвести включение тестовой программы.

Для исследования ПЭМИН монитора применяют программу WTEST, которая представляет собой файл с расширением .exe, после запуска которого на экране монитора отображается окно, изображенное на рисунках 20 и 21.

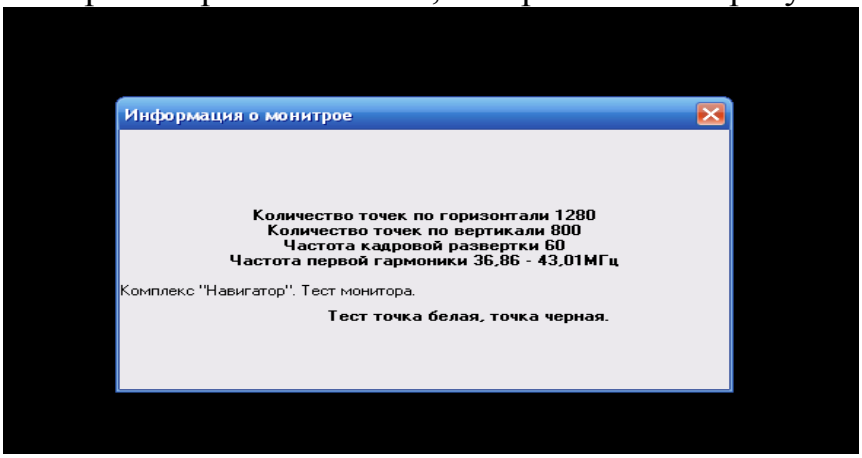


Рис. 20. Запуск тестовой программы.

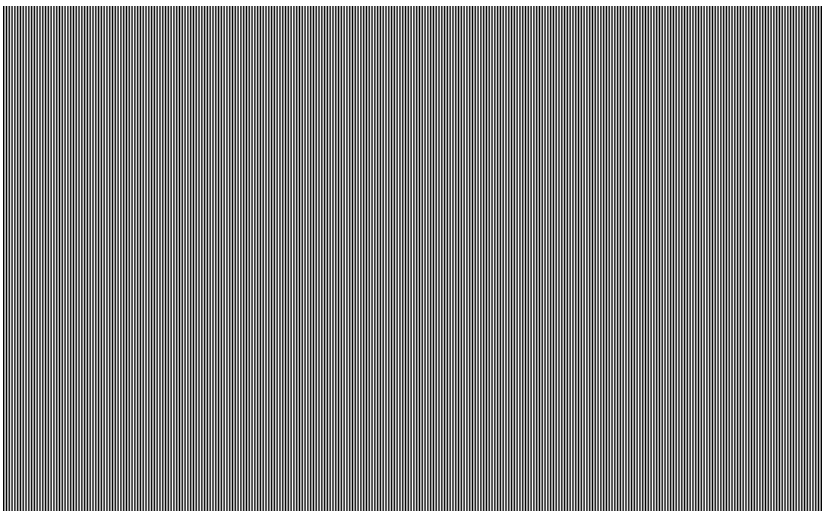


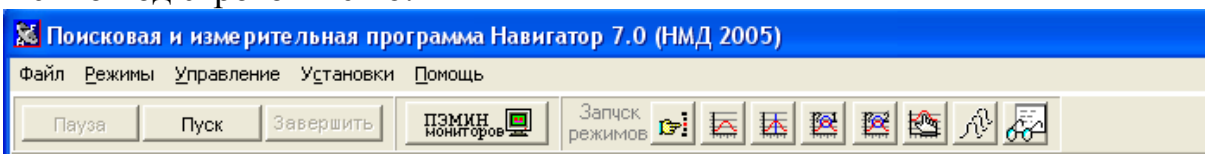
Рис. 21. Запуск тестовой программы.

Последующие действия оператора состоят в последовательном включении и выключении (нажатие пробела или клик мышкой) теста по требования программы «Навигатор».

6. Запустить поисковую и измерительную программу «Navigat.exe».

Рис. 22. Запуск программы «Navigat.exe».

Управление работой программы осуществляется через меню программы, а также с помощью кнопок строки управления, находящихся непосредственно под строкой меню:



При первом запуске программы или в случае замены измерительного оборудования в режиме "Настройка: оборудование, антенны, частотные диапазоны" необходимо выбрать используемое оборудование и интерфейс управления прибором (Рис.23).

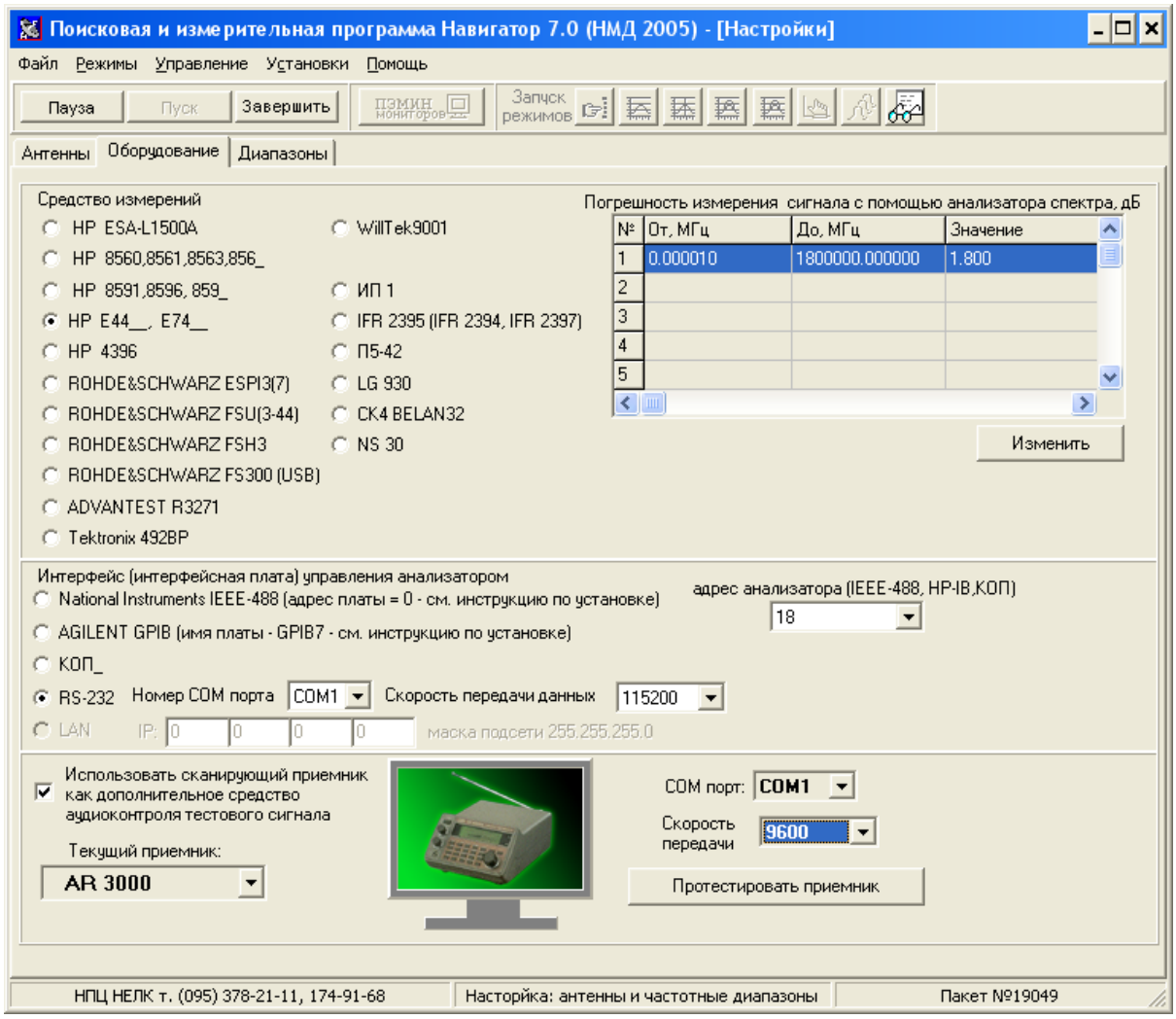


Рис. 23. Настройка программы.

7. Раскрыть пункт меню «Установки». Напротив подпункта "Демонстрационный режим" (в этом режиме данные об электромагнитной обстановке эмулируются программой) убрать маркер «галочка», т.к. программа работает с реальным оборудованием (Рис.24).

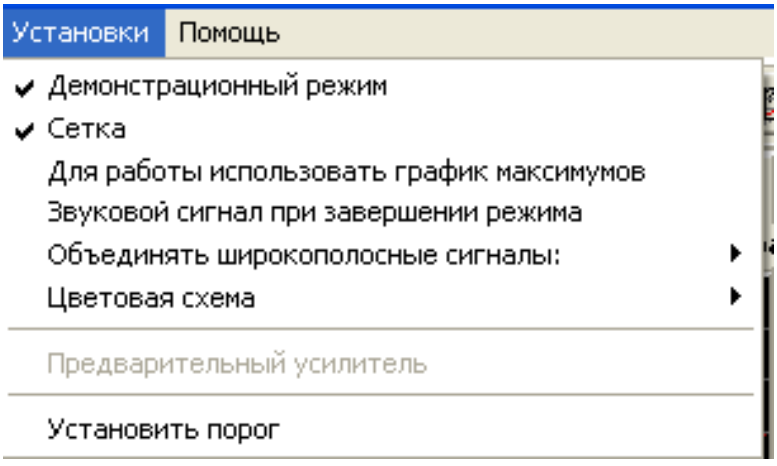


Рис. 24. Настройка программы.

8. Занести данные о новых антеннах в таблицы на странице «Антенны» в случае использования новых антенн.

8.1. Выбрать режим «Настройка: оборудование, антенны, частотные диапазоны».

8.2. Выбрать страницу «Антенны» (Рис.25).

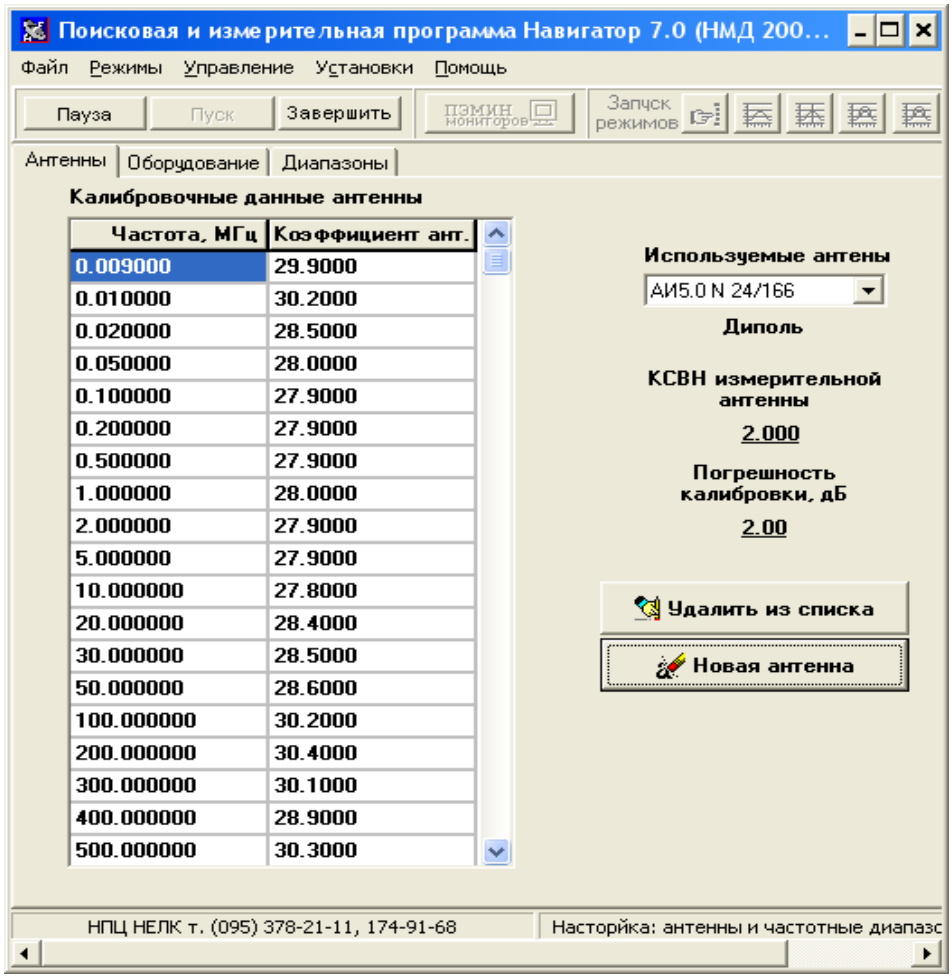


Рис. 25. Калибровка антенны.

Данные об используемой антенне достаточно один раз занести в программу и далее антенну можно использовать по данному ей символическому имени. В качестве антенны могут выступать токосъемники или эквивалент сети (для измерения наводок в цепях).

9. Нажать кнопку "Новая антенна" для занесения данных о новом оборудовании.

В раскрывающемся диалоговом окне заполнить таблицу калибровочных коэффициентов (частота/коэффициент антенны), погрешность калибровки, КСВН антенны (в данной версии ПО этот показатель не используется, рекомендуется заносить значение "2"), ввести имя антенны, а из раскрывающегося списка выбрать тип антенны (Рис.26).

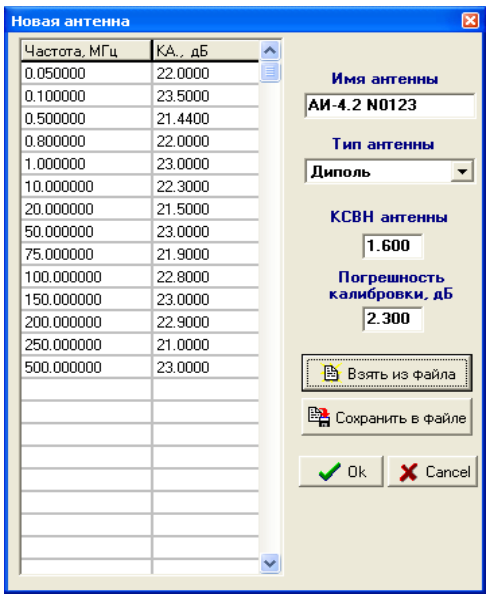


Рис. 26. Настройка антенны.

10. Перейти на страницу "Диапазоны" режима "Настройка: анализаторы, антенны, частотные диапазоны" и создать задание на исследование (Рис.27).

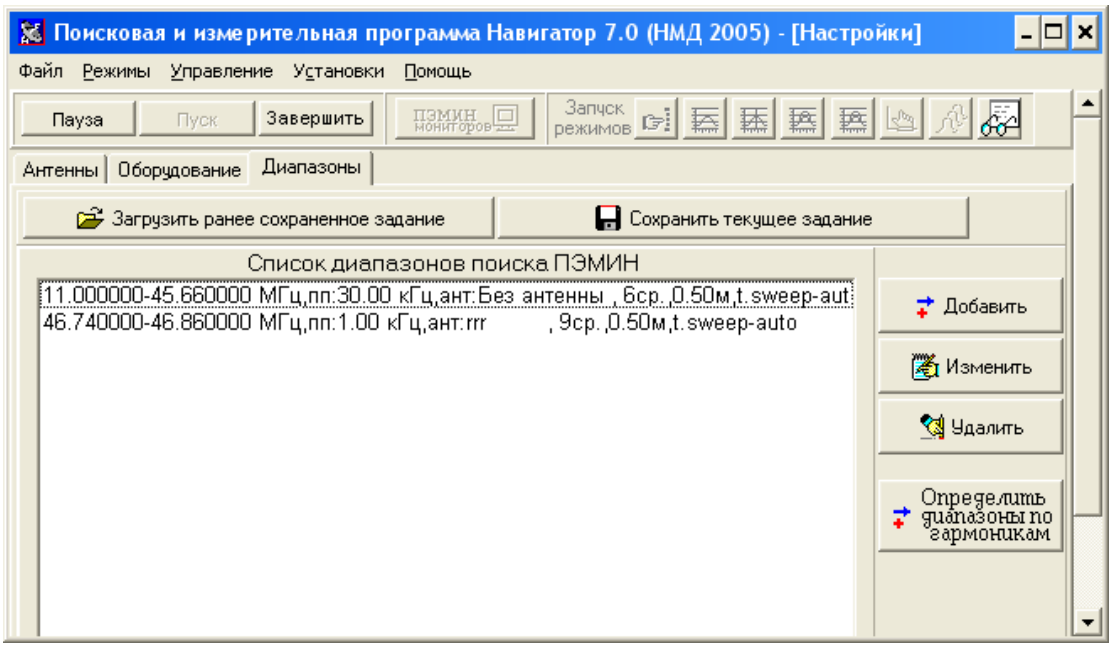


Рис.27. Создание задания на исследование.

10.1. Нажать на кнопку «Добавить» (Рис.28).

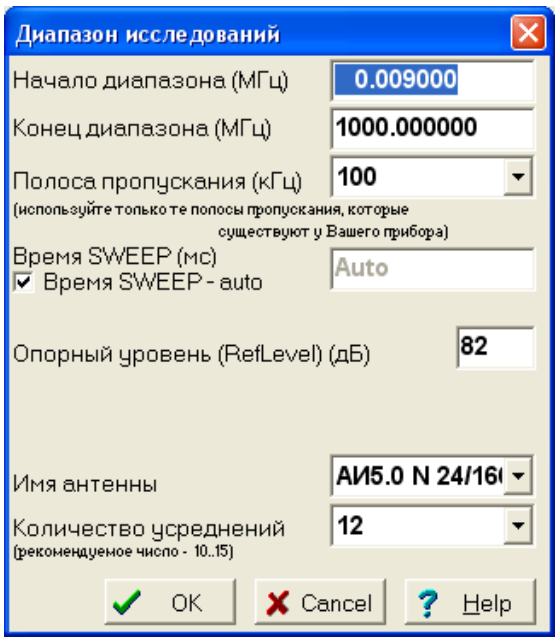


Рис.28. Задание исследования.

В низкочастотном диапазоне необходимо использовать узкие полосы пропускания, а в высокочастотном диапазоне можно использовать более широкие полосы пропускания для уменьшения времени поиска. Предлагается следующий вариант диапазонов и полос пропускания:

Диапазон, МГц	Полоса пропускания, кГц
до 3	1
от 3 до 100	10 или 30
от 100	100

Если сигналы ПЭМИН не найдены или исследуемая аппаратура выполнена в защищенном исполнении, то необходимо повышать чувствительность - уменьшать полосы пропускания.

Параметр "Время SWEEP" определяет время сканирования заданной полосы обзора анализатором спектра. Минимально корректное значение времени сканирования устанавливает сам анализатор при постановке галочки в поле «Время SWEEP – auto».

Для анализатора спектра необходимо стремиться к тому, чтобы информация о спектре занимала не менее 80% области экрана по амплитуде, поэтому опорный уровень выставляется в районе 80 дБ.

Усреднение позволяет существенно снизить уровень шума и выделить те сигналы, которые при однократных измерениях были скрыты шумовой дорожкой.

11. Для обнаружения ПЭМИН установить измерительную антенну в непосредственной близости от исследуемого источника излучения. Сформи-

ровать список сигналов. Выключить тест на исследуемом оборудовании и запустить режим "Измерение индустриального шума" (Рис.29).

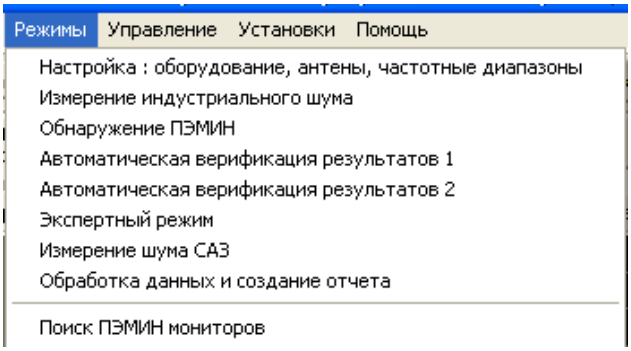


Рис. 29. Измерение индустриального шума.

11.1. Установить необходимое значение порога обнаружения (3-6 дБ) (Рис. 30, 31).

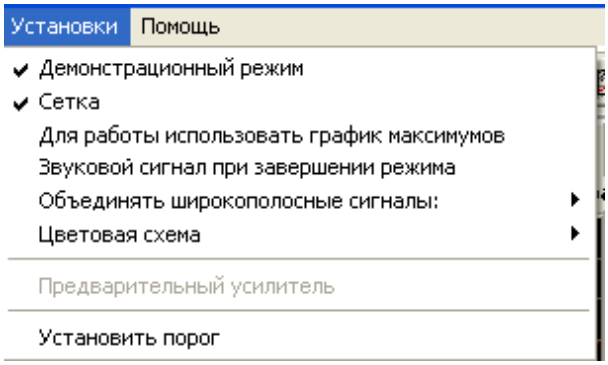


Рис. 30. Установка порога обнаружения.

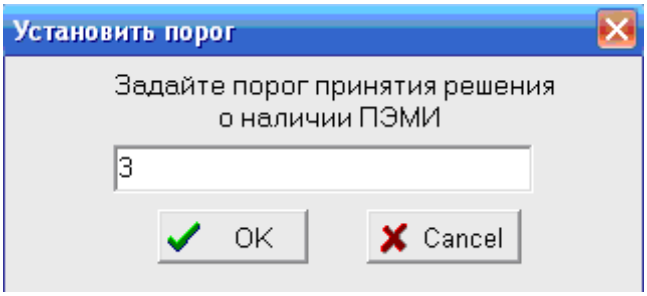


Рис. 31. Установка порога обнаружения.

12. Включить тест на исследуемом оборудовании и запустить режим "Обнаружение ПЭМИН".

После завершения работы режима "Обнаружение ПЭМИН" в правой части программы будет сформирован список сигналов, имеющих превышение над уровнем шума на установленный порог при включенном тестовом сигнале. Голубым цветом отображается индустриальный уровень шума около контролируемой точки, желтым – индустриальный уровень шума с наложенными на него сигналами ПЭМИН (Рис.32).

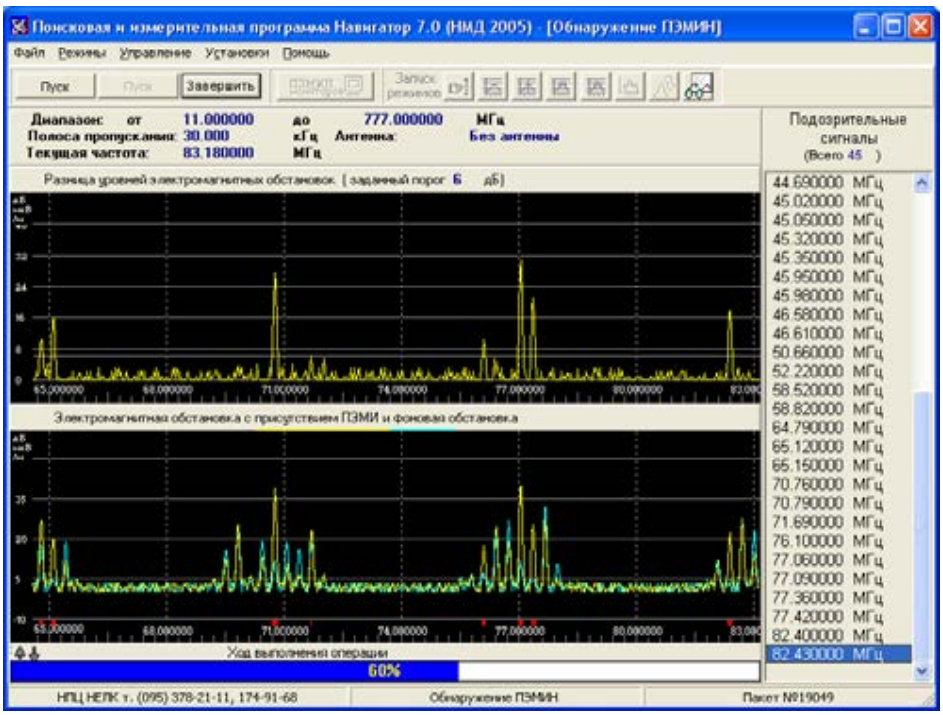


Рис. 32. Результаты обнаружение ПЭМИН.

Запустить режим "Автоматическая верификация результатов 1"(с включенным тестом) и "Автоматическая верификация результатов 2" (с выключенным тестом) для удаления программой сигналов из списка частот, не являющихся ПЭМИН (Рис.33).

В поле «Задано циклов верификации» следует установить число, не менее 2.

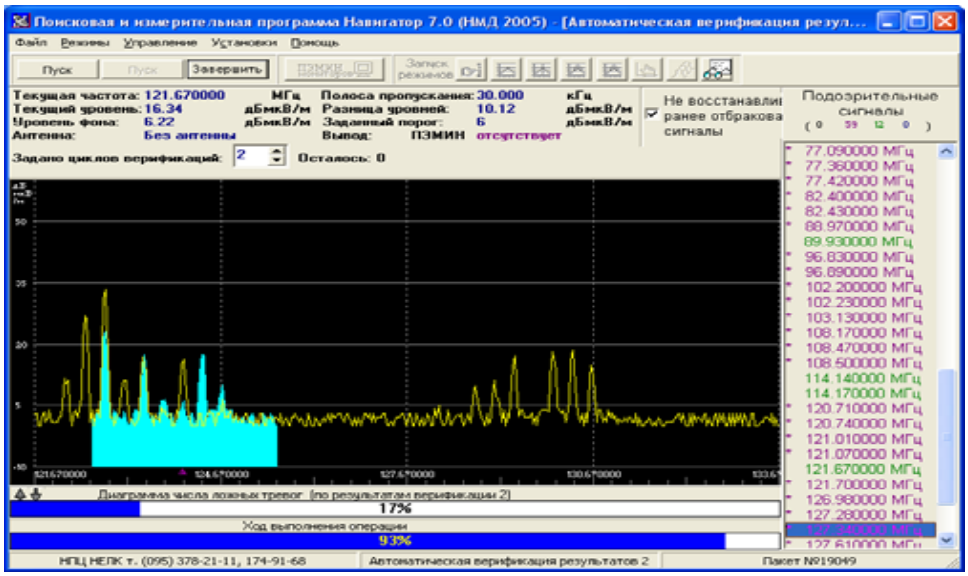


Рис. 33. Запуск верификации.

13. Перейти в «Экспертный режим» (Рис.34).

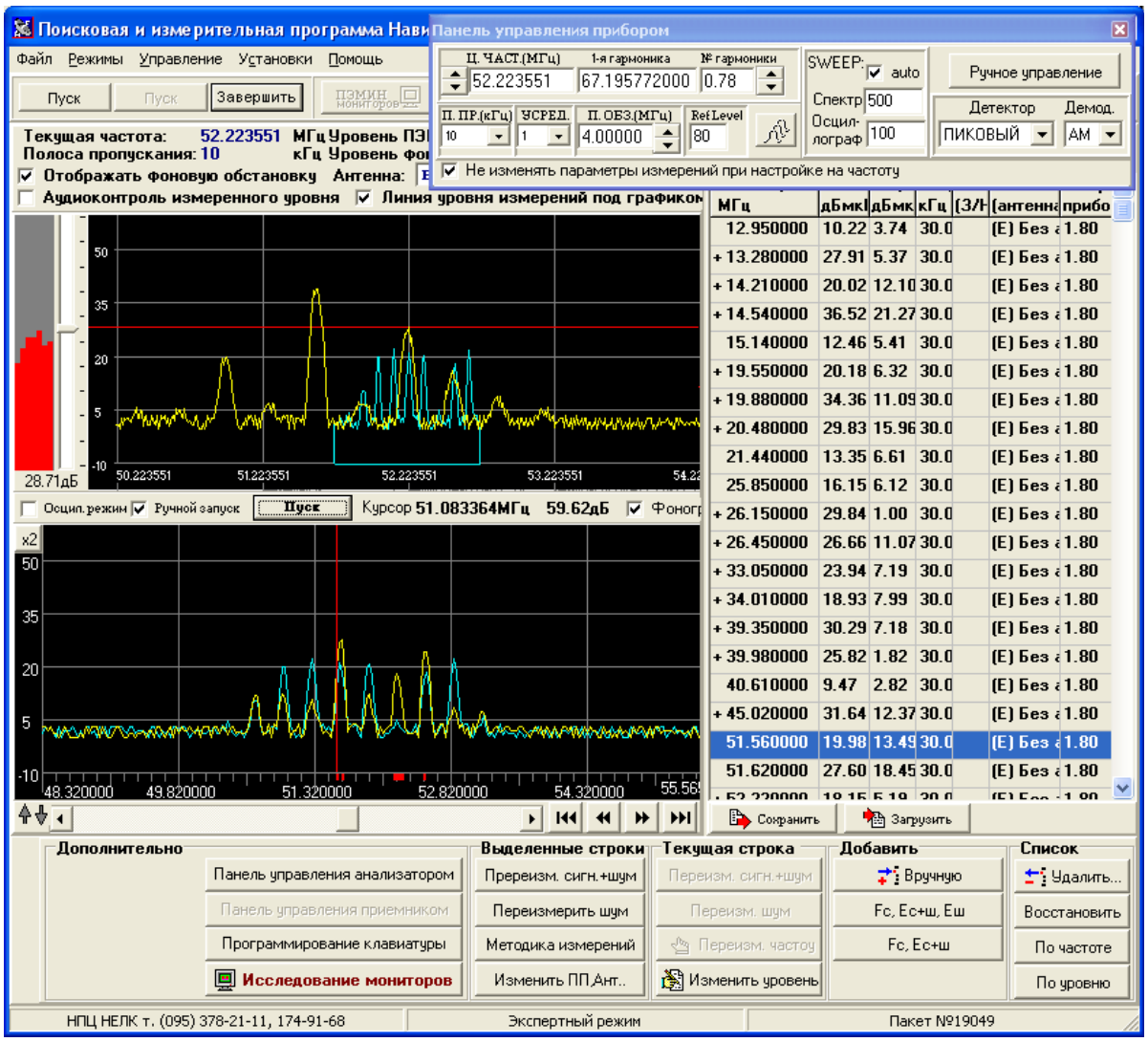


Рис. 34. Экспертный режим.

14. Выбрать осциллографический режим работы анализатора.

15. Нажать кнопку «Панель управления анализатором» в нижней части окна.

В диалоговом окне появится виртуальная панель управления анализатором спектра (Рис.35).

Рис. 35. Панель управления анализатором спектра.

В поле «1-я гармоника» ПАК «Навигатор» самостоятельно определил значение частоты первой гармоники, которое зачастую является неверным. Необходимо уточнить это значение.

16. Установить удобный масштаб отображения графиков с помощью кнопок масштабирования.

Просматривать частотный диапазон от начала, прокручивая кнопки , при этом наблюдать за изменением спектрограмм в верхней части окна.

При изменении формы сигнала в вид меандра, можно сделать вывод, что данная частота является частотой первой гармоники тест-сигнала.

Убедиться в правильности такого предположения можно следующим образом: выключить тест-сигнал, посмотреть на верхний график: форма меандра должна измениться.

Уничтожить все обнаруженные сигналы в списках нажатием на кнопку «Удалить».

Нажать на кнопку 

В появившемся окне установить число 1 (текущая частота является частотой 1-й гармоники), нажать кнопку «Сохранить» (Рис.36).

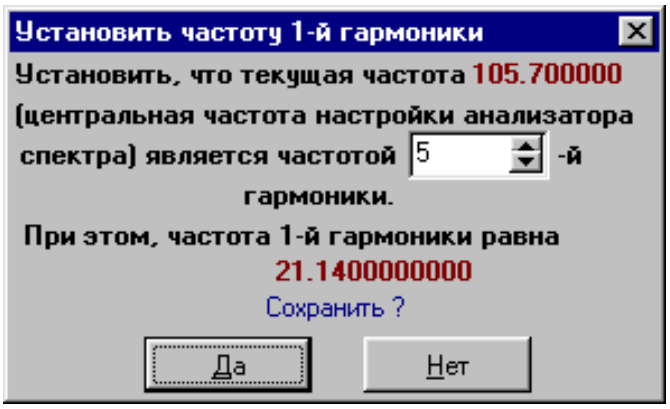


Рис. 36. Установка частоты 1-й гармоники.

Нажать кнопку 

, появится окно, изображенное на рисунке 37.

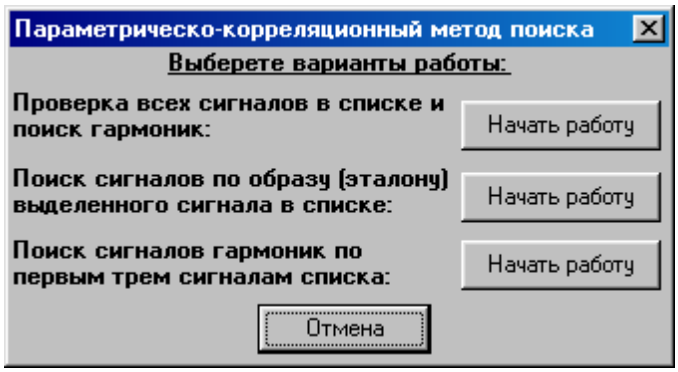


Рис. 37. Выбор вариантов работы.

Нажать на кнопку «Начать работу» в строке «Поиск сигналов по образу (эталону)» и следовать указаниям программы (включать-выключать тест сигнал). Далее появятся окна изображенные на рисунке 38 и 39.

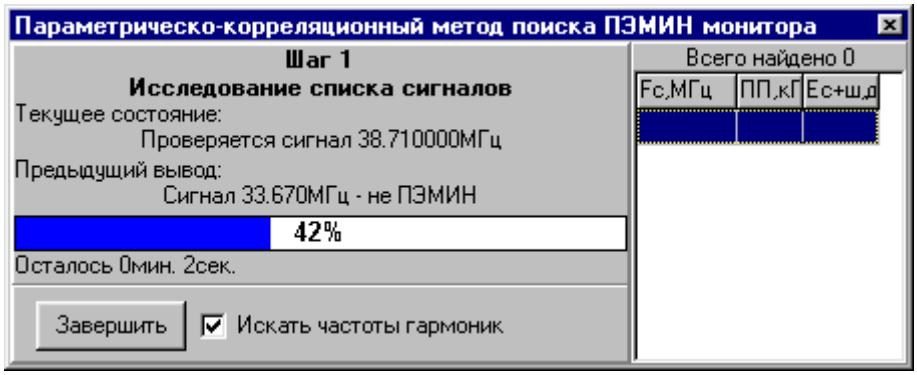


Рис. 38. Исследование списка сигналов.

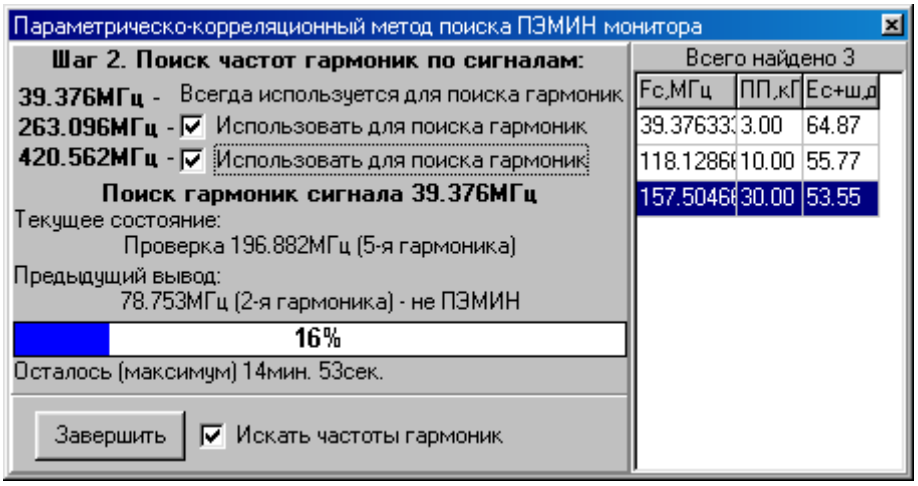


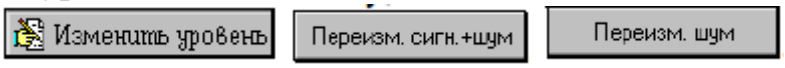
Рис. 39. Поиск гармоник сигналов.

По завершению работы данного алгоритма будет сформирован список частот, на которых присутствуют ПЭМИН. Необходимо сохранить результаты обнаружения сигналов в файле или в отчете поиска сигналов ПЭМИН с отметкой "Найденные сигналы".

17. Далее следует установить антенну на расстояние корректного измерения. Расстояние корректного измерения в соответствии с НМД - 1 метр от поворотного стола. Измерить амплитуду сигналов и уровень шума на корректном расстоянии. Перейти в «Экспертный режим» и вращать платформу стола вокруг неподвижно установленной антенны.

Изменять высоту поднятия антенны нельзя!

Если сигнал на расстоянии измерения или при использовании другой полосы пропускания не обнаружен, то это означает, что шум при данных условиях приема выше, чем уровень сигнала. В этом случае за амплитуду сигнала необходимо принимать значение уровня шума, а уровень шума необходимо установить на 6 дБ меньшим, чем уровень сигнала.

18. Настроиться на частоту исследуемого сигнала путем двукратного нажатия левой кнопкой мышки на требуемой строке списка ПЭМИН. Занести максимальный из выявленных уровень сигнала вместо имеющегося значения в списке с помощью кнопок 

Для автоматизации процесса в «Навигаторе» существует механизм аудиоконтроля.

Для его активизации необходимо поставить галочку в поле 

. После этого каждое измерение сопровождается воспроизведением звукового значения через динамики компьютера.

19. Запустить расчетную программу "NavigatC.exe", выбрав режим "Подготовка данных и создание отчета" и определить необходимые параметры на странице "Параметры". При необходимости заполнить данные на других страницах таблицы режима.

В группе полей выбора "Решаемая задача" выбрать ту задачу, для которой необходимо произвести расчет параметров.

В группе полей редактирования "Параметры тестового сигнала" определить параметры тестового сигнала: тактовую частоту тестового сигнала, длительность импульса тестового сигнала, тип кодирования, число разрядов (только для параллельного кода).

При нажатии клавиши "Enter" когда курсор установлен в поле "Тактовая частота", значение длительности импульса автоматически рассчитывается для меандра исходя из значения тактовой частоты.

В группе полей редактирования "Нормированные отношения с/ш" ввести одноименные показатели применительно к типу исследуемого ТС из «Норм защиты информации, обрабатываемой средствами вычислительной техники и в автоматизированных системах от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)» (Рис.40).

При решении задач специальных исследований и контроля наводок значения группы полей редактирования " Расстояния, м. " не используются.

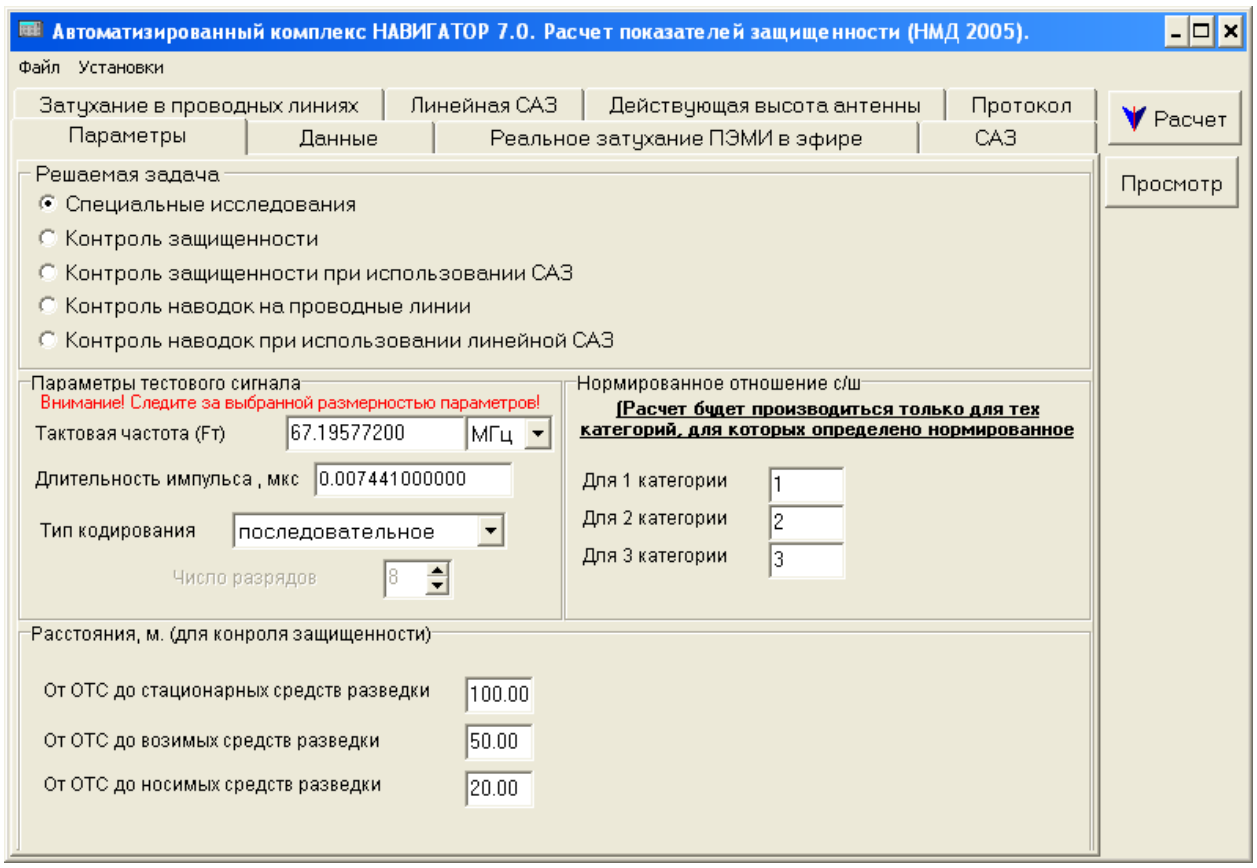


Рис. 40. Настройка программы.

Провести расчет (кнопка "Расчет"). Сохранить протокол в виде файла для отложенного редактирования. В раскрывшемся окне редактирования отчета (или в Microsoft Word) отредактировать протокол расчета в соответствии с требованиями.

6. Использование специальных знаний при проведении специальных мероприятий в области обеспечения информационной безопасности.

Подготовка к специальным мероприятиям.

Важным аспектом проведения специальных мероприятий является использование специальных знаний направленных на получение сведений об инциденте в сфере информационной безопасности.

Помимо стандартных действий, которые необходимо выполнить при подготовке к проведению специальных мероприятий связанных с осмотром средств вычислительной техники, следует установить:

– количество компьютерной техники её тип и расположение;
– наличие автономных источников питания;
– используемые электронные носители информации;
– наличие систем экстренного уничтожения данных.
– используемое программное обеспечение;

– количество компьютеров и их распределение по службам и помещениям;

– объединены ли компьютеры в локальную сеть.

Если такое объединение существует, то необходимо установить:

– ответственных за сетевую систему и программное обеспечение, т.е. администраторов системы;

– количество и типы используемых серверов;

– количество и типы рабочих мест;

– типы используемых операционных сетевых систем;

– прикладное программное обеспечение, используемое в сети (например, сетевые базы данных, система документооборота и пр.);

– наличие резервных копий серверных дисков и баз данных и место их хранения;

– наличие выхода в другие, в том числе и глобальные, сети;

– используются ли распределенные сети или почтовые программы для связи с удаленными подразделениями организации или с другими предприятиями;

– используются ли системы шифрования и защиты информации; если да, то какие;

– используются ли другие средства компьютерной связи (например, модемы и радиомодемы, выделенные линии);

– наличие выхода в сеть Интернет (данные провайдера предоставляющего услуги выхода в сеть интернет);

– расположение систем вентиляции и кондиционирования (актуально для серверных помещений);

– план-схема помещений.

Определение обстоятельств установки и использования программных продуктов и оборудования.

К данному пункту можно отнести:

- исследование установленного контрафактного обеспечения;
- параметры и регистрационные данные программного обеспечения;
- следы использования программного обеспечения и оборудования.
- наличие систем защиты информации и шифрования, их типы.

Проведение специальных мероприятий

При проведении специальных мероприятий связанных с участием специалиста основной задачей применительно к компьютерным средствам является обеспечение сохранности информации, имеющейся в компьютерах и на компьютерных носителях информации. Для этого, в зависимости от обстоятельств дела, необходимо:

– предотвратить отключение энергоснабжения предприятия, обеспечив охрану распределительного щита.

(в случае выполнения операций или наличия, не сохранённого файла, такая информация теряется)

– запретить производить какие-либо манипуляции с компьютерами и носителями информации, даже членам следственной группы, все действия выполнят специалист, в случае невозможности специалиста провести действие, оно выполняется под его контролем;

– оградить работающие компьютеры от случайных нажатий на клавиши клавиатуры, кнопок системных блоков и устройств;

– предупредить всех сотрудников о недопустимости самостоятельной манипуляции с компьютерной техникой и носителями информации;

– удалить из помещений, в которых находятся компьютеры и носители информации, все взрывчатые, едкие и легковоспламеняющиеся материалы;

– обеспечить отключение беспроводных систем передачи данных.

(При соблюдении это пункта следует иметь в виду, что некоторая информация может обрабатываться на удалённом сетевом ресурсе, в этом случае следует принять меры к сохранению такой информации с фиксацией данных сетевого ресурса, на конкретный момент времени.)

При наличии в осматриваемом помещении локальной сети необходимо точно установить местоположение серверов. Как правило, для расположения серверов выделяют специальное помещении, вход в которую ограничен. Следует помнить, что серверы требуют наличие систем охлаждения. Однако помимо центральной серверной в отделах могут находиться местные локальные серверы. Определить местоположение компьютеров при наличии локальной сети можно с помощью проводки. Достаточно проследить трассы кабеля или коробов (в случае, когда кабель спрятан в специальный короб), а так же наличия беспроводных сетей.

(Наличие беспроводных сетей можно определить любым устройством (мобильный телефон, планшетный компьютер и т.д.) имеющем соответствующие возможности по беспроводному сетевому соединению).

Следует обратить внимание на содержимое мусорных корзин, надписей и наклеек на мониторе и системных блоках, т.к. там могут содержатся данные о пароле и учетном имени (логине) пользователя.

Особое внимание нужно обратить на места хранения внешних носителей информации, данные о подключении таких носителей содержатся в служебных файлах и реестре операционной системы. Надо иметь в виду, что в качестве носителей информации могут выступать, например фоторамки, плееры, и другие мультимедийные устройства.

На предприятиях, имеющих развитую локальную сеть, как правило, производится регулярное архивирование информации на какой-либо носитель, поэтому необходимо определить место хранения данных копий.

Обязательно следует выявить администратора системы и провести его опрос, при котором выяснить следующее:

– какие операционные системы установлены на каждом из компьютеров;

– какое программное обеспечение используется;

– какие программы защиты и шифрования используются;

– где хранятся общие файлы данных и резервные копии;

– пароли супервизора и администраторов системы;

– имена и пароли пользователей.

Далее специалист, участвующий в проведении специальных мероприятий, используя данные, полученные от администратора системы, может произвести копирование информации на заранее приготовленные носители.

Возможности использования средства экстренного уничтожения компьютерной информации.

Способы уничтожения информации на накопителях на жестких магнитных дисках (далее НЖМД)можно разделить на три группы.

1. Программные, в основу которых положено уничтожение записанной на НЖМД информации, посредством многократной перезаписи, как правило, для таких целей используют специализированное программное обеспечение. Следует иметь в виду, что это длительный процесс, так как требуется не менее чем троекратная перезапись. На время процесса существенное влияние оказывает и объем уничтожаемой информации. Важным является то, что в случае наличия неисправностей НЖМД провести надежное уничтожение информации невозможно.

При многократной перезаписи уровень магнитного поля головки чтения-записи меньше уровня насыщения магнитной среды, поэтому полностью стереть информацию невозможно, при использовании специальных высокочувствительных считывающих головок или с помощью визуализации возможно восстановить такую информацию.

2. Механические, связанные с механическим разрушением рабочей поверхности магнитного диска. Следует знать, что повреждения корпуса НЖМД, элементной базы, или механизма считывания не гарантируют уничтожение информации. К механически средствам воздействия относят так же пиротехнические (взрыв), химические (кислоты, щелочи или иные химически активные вещества) и термические способы воздействия, (нагрев). При термическом способе воздействия для достижения требуемого эффекта должна быть достигнута температура перехода через точку Кюри. Производители держат эти данные в секрете, но это не менее 800-1000 °С. Следовательно после пожара, максимум температуры прядка 900°С достигается в очаге, имеется большая вероятность того, что информацию с НЖМД возможно считать. Как показывает опыт сделать это возможно даже без использования специального оборудования.

3. Физические, связанные с физическими принципами формирования записи на магнитном носителе, и основанные на перестройке доменной структуры рабочих поверхностей магнитного диска. Для этого применяют либо размагничивание либо намагничивание носителя до максимального значения (насыщения).

Реализация первого способа (размагничивания) технически сложный и длительный процесс, так как требует наличия магнитов специальной формы и большой напряжённостью электромагнитного поля.

При способе, использующем избыточное намагничивание происходит изменение размеров магнитных доменов и их ориентации, что приводит к разрушению доменной структуры магнитного слоя и невозможности считывания информации. Кроме того при таком воздействии происходит уничтожение разметки поверхности диска и данных в служебных секторах. При этом нарушается работоспособность самого НЖМД из-за отсутствия служебной разметки диска и управляющих механических процессов.

Способы воздействия на накопитель:

- без разрушения корпуса поверхностей НЖМД;
- с разрушением корпуса НЖМД.

Пример системы гарантированного уничтожения данных путем избыточного намагничивания.

Система состоит из трёх основных компонентов:

- накопитель заряда;
- камера стирания;
- управляющий модуль.

Накопитель заряда, предназначен для накопления электромагнитного импульса достаточного для уничтожения данных на диске. Может работать как от сети, так и от батареи. Время зарядки около 2-4 сек..

Камера стирания - место, куда помещается НЖМД предназначенный для уничтожения.

Управляющий модуль служит для принятия и исполнения команд на уничтожение информации.

Рис. 41. Внешний вид устройства уничтожения информации

Команды на уничтожения могут подаваться как по радио тракту, например брелока автосигнализации или с использованием GSM-модулей. Так же предусмотрены возможности активации и со встроенных датчиков, например при вскрытие корпуса или перемещение.

Ниже на рисунки приведены примеры видимого изображения визуализации рабочей поверхности магнитного носителя до и после применения системы уничтожения данных.

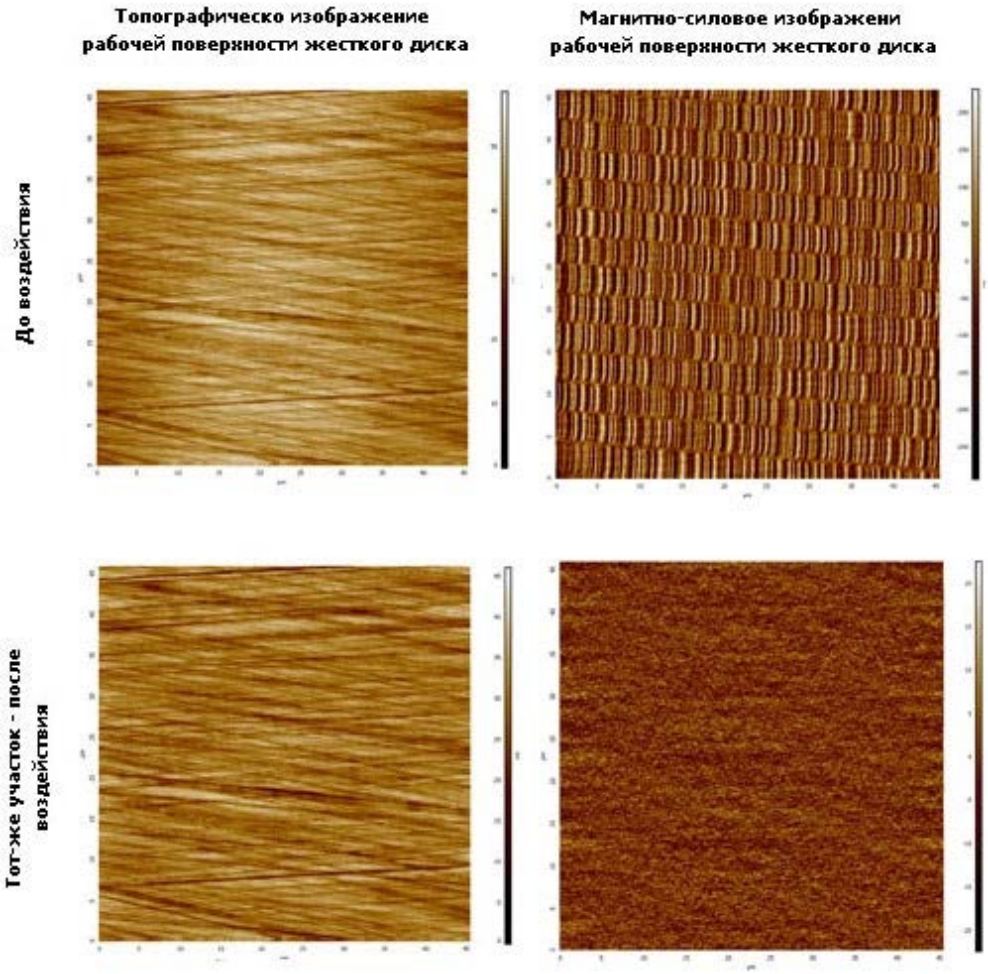


Рис. 42. Изображения визуализации рабочей поверхности магнитного носителя до и после применения системы уничтожения данных.

Изъятие средств вычислительной техники и носителей информации

При изъятии средств вычислительной техники и носителей информации:

– опросить персонал порознь, выяснить сетевые имена пользователей и их пароли;

– изъять все компьютеры и носители информации;

– при осмотре документов обратить особое внимание на рабочие записи сотрудников, где могут содержаться пароли и коды доступа;

– составить список всех нештатных и временно работающих специалистов фирмы с целью обнаружения программистов и других специалистов по вычислительной технике, работающих на данную фирму. По возможности установить их паспортные данные, адреса и места постоянной работы.

При осмотре должны быть установлены:

– конфигурация компьютера (с четким описанием всех устройств);

– номера моделей и серийные номера каждого из устройств;

– инвентарные номера, присваиваемые бухгалтерией при постановке оборудования и программного обеспечения на баланс предприятия;

– прочая информация, имеющаяся на фабричных ярлыках.

Кроме того, все изъятые системные блоки должны быть опечатаны таким образом, чтобы исключить возможность их включения и разборки.

Обеспечение неизменности информации на электронных носителях.

При работе с компьютерными носителями информации важно обеспечение неизменности информации на осматриваемом электронном носителе информации, например НЖМД - накопителях на жестких магнитных дисках, различных flech - носителях и т.п.

Самым приемлемым, в простоте и затрате времени и материальных средств, следует признать блокировку записи по USB - порту, при подключении через данный интерфейс исследуемых носителей. При этом необходимо наличие переходных устройств HDD – USB адаптеров, например SATA - USB или IDE - USB. И соответствующего, бесплатного для силовых органов, программного обеспечения, например "NCFS SoftwareWrite-block XP", либо отключать запись по USB порту в реестре изменением значения "WriteProtect". Надо иметь в виду, что последний способ позволяет блокировать запись и в операционной системе Windows 7. Однако данные ключи по умолчанию в реестре не существуют их необходимо создавать вручную или создать соответствующие файлы для активации или дезактивации этих функций. Для вступления в силу изменений достаточно подключить носитель информации.

Данные реестра для блокировки записи:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]

"WriteProtect"=dword:00000001

Данные реестра для снятия блокировки записи:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]

"WriteProtect"=dword:00000000

Для надежной блокировки, с наименьшими затратами возможно использование HDD – USB адаптеров с функцией блокировки записи, такие устройства выпускает компания AGESTAR. Внешний вид одного из адаптеров приведён ниже на рисунке.

Рис. 43. Внешний вид адаптера с возможностью блокировки записи

Дальнейшая работа возможна как непосредственно с исследуемым носителем информации, так и с созданным посекторной копией или образом. Предпочтительнее в дальнейшем исследовании использовать именно образ или посекторную копию предоставленного носителя информации, в том числе это позволит избежать возможных дефектов связанных с эксплуатацией носителя информации. Тем более, что полученную посекторную копию возможно использовать как непосредственно для запуска с исследуемого системного блока или ноутбука, так и для запуска в виртуальных средах (виртуальных машинах). Для запуска в виртуальных машинах подходят так же и полученные образы носителей информации. Современные средства создания образов, например продукты компаний «Acronis» или «ParagonSoftwareGroup» позволяют создавать сразу образы носителей информации в форматах распространённых виртуальных машин. Пожалуй, продукты «Acronis» несколько предпочтительней, так как имеется возможность запуска продукта с внешнего носителя на ядре Linux.

Ниже перечислены наименования и возможности некоторых продуктов «Acronis»

AcronisBackup&Recovery — линейка решений для резервного копирования и аварийного восстановления данных, включающее как серверные решения, так и решения для рабочих станций. Возможно клонирование разделов НЖМД, а так же создание образов, в том числе совместимых с виртуальными машинами.

AcronisTrueImageHome — линейка решений для резервного копирования и аварийного восстановления данных для домашних пользователей.Возможно клонирование разделов НЖМД, а так же создание образов, в том числе совместимых с виртуальными машинами

AcronisvmProtect — решение для резервного копирования и восстановления сред VMwarevSphere.

AcronisDiskDirector — линейка решений по управлению разделами и обслуживанию жестких дисков. Возможно клонирование разделов НЖМД.

AcronisSnapDeploy — линейка решений для быстрой установки ПОна новые компьютеры при помощи технологии создания образов дисков.Возможно клонирование разделов НЖМД, а так же создание образов, в том числе совместимых с виртуальными машинами.

AcronisMigrateEasy — решение для клонирования данных с одного жёсткого диска на другой.

При создании образов носителей информации необходимо использовать режим посекторного резервного копирования с функцией копирования нераспределённого пространства. При использовании этого способа возможно использовать подключённый образ для восстановления удаленной информации.

Естественно возможно использование и других программных решений, как для сред Windows так и для unix, (загрузочные носители на базе специализированных продуктов). В состав должно входит следующее программное обеспечение.

Анализаторы беспроводных сетей, в том числе предназначенные для перехвата передаваемого через беспроводные сети трафика.

Инструмент для создания, тестирования и использования эксплойтов.

Утилиты, предназначенные для сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб).

Программно-аппаратный комплекс PC-3000.

Программно-аппаратный комплекс PC-3000 позволяет создавать копии данных, в том числе с неисправных носителей информации (НЖМД). Для этого с помощью входящих в набор технологических переходников и адаптеров осуществляется подключение НЖМД. После определения данных о подключенном НЖМД с помощью программы "DataExtractor"входящей в состав комплекса выбирается режим "Создание копии данных" с выбором способа создания, либо образ файловой системы, либо посекторное копирование на выбранный НЖМД. Программа "DataExtractor" позволят также подключать исследуемые носителе информации в безопасном режиме, «создание виртуального транслятора».

Комплекс PC-3000 позволяет восстановить информацию с поврежденных носителей в следующих случаях:

"- повреждения поверхности или блока магнитных головок;

- разрушения "служебной информации", приводящие к неустойчивому чтению и множественным ошибкам;

- нарушение системы сопоставления логического дискового пространства (LBA) с физической геометрией НЖМД (транслятора)."

При восстановление информации с повреждённых носителей, при использовании PC-3000, необходимо учитывать характеристики НЖМД конкретных производителей. Для каждого НЖМД конкретных производителей имеется соответствующий набор специализированных утилит. Полное использование комплекса требует наличия определенной подготовки и знаний аппаратной и технической части НЖМД, однако использование комплекса для восстановления информации, в ряде некритичных случаев (поломок НЖМД) затруднений не вызывает.

После производства специальных мероприятий связанных с изятием информации необходимо произвести специальное исследование компьютерной информации. При производстве специального исследования компьютерной информации решают следующие задачи.

Поиск информации.

Определение обстоятельств установки и использования программных продуктов и оборудования.

К задачам поиска информации относят:

- поиск текстовой информации по ключевым словоформам;
- поиск графической информации по заданным критериям;
- поиск текстовой и графической информации по соответствию предоставленным образцам;
- поиск информации о сетевых подключениях (выход в сеть "internet");
- поиск программных продуктов и др.

Поиск текстовой информации проводился по ключевым. Для поиска текстовой информации используются специализированное программное обеспечение «Terrier», стандартные средства поиска "Windows", программы "Архивариус3000", "AVSearch 3.12a" и встроенные средства поиска файловых менеджеров. Для более глубокого анализа можно использовать специализированное программное обеспечение для проведения криминалистических исследований, например «Belkasoft».

Поиск графической информации проводится путем просмотра графических файлов. Важно заметить, что изображения так же могут содержаться, например, в файлах созданных приложениями Office, однако данные файлы графическими являться не будут. С помощью программ поиска текстовой информации, возможно, искать графические файлы, например содержащие информацию EXIF. При этом возможно установить графические файлы, созданные с помощью определённых моделей цифровых фотоаппаратов или камер мобильных телефонов.

Для поиска графической информации с помощью "Архивариус 3000" возможно вводить в поисковый запрос сведения EXIF цифровой фототехники, например модель или серийный номер цифровой фотокамеры. Так же возможен поиск по расширению файлов. Найденные файлы копируются на стендовый носитель, для дальнейшего исследования (просмотра).

Определение обстоятельств установки и использования программных продуктов и оборудования.

К данному пункту можно отнести:

- исследование установленного программного обеспечения;
- параметры и регистрационные данные программного обеспечения;
- следы использования программного обеспечения и оборудования.

В среде "Windows" большинство основных данные об установленном программном обеспечении и оборудование хранится в реестре.

Для определения проведённых действий операционной системой семейства "Windows" производится просмотр журнала событий операционной системы содержащихся в файлах «SysEvent.Evt» и «AppEvent.Evt» расположенных в директории «:\WINDOWS\system32\config\» для WindowsXP и в файлах «Application.Evtx» и «System.Evtx» расположенных в директории %SystemRoot%\System32\Winevt\Logs\ для Windows 7 и выше.

Просмотром данных журналов возможно определить:

- временные рамки работы операционной системы;
- временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале событий операционной системы "Windows";
- временные рамки подключения - отключения сетевых ресурсов (сетевого адаптера) запуск которых отображается в журнале событий операционной системы "Windows", и ряд других параметров.

Для определения сведений об операционной системе следует использовать данные из реестра. Данные реестра содержащие сведения об операционной системе хранятся в ветви реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Current Version

Где содержатся сведения о наименовании операционной системы.

Дата инсталляции InstallDate (дата инсталляции дата установки операционной системы хранится в шестнадцатеричном и десятичном виде). Параметр InstallDate показывает количество секунд, прошедших с 1 января 1970 г. до момента установки операционной систем.

Идентификационные номера продукта и пути установки.

Если система находится в активном состоянии, включена, то используют данные полученные с помощью команды: "systeminfo".

Информация о подключенных внешних устройствах хранится в реестре операционных систем, журналах событий и в файле «setupapi.log» расположенном в директории «Windows» для «Windows XP» и в файле «setupapi.dev.log» расположенном в директории \Windows\inf\ для "Windows 7".

Данные из реестра:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB

И

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

В данных ветвях содержится информация о типе и виде подключенных устройств, а так же их серийный номер и уникальный номер (Globally Unique Identifier - GUID), который идентифицирует устройство для системы.

Причем данные о серийном номере содержатся в имени ветви, например:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB\Vid_058f&Pid_6387\FKZ9XO6P где FKZ9XO6P серийный номер устройства.

Ниже на рисунке 44 приведены данные из реестра о подключении внешних устройств.

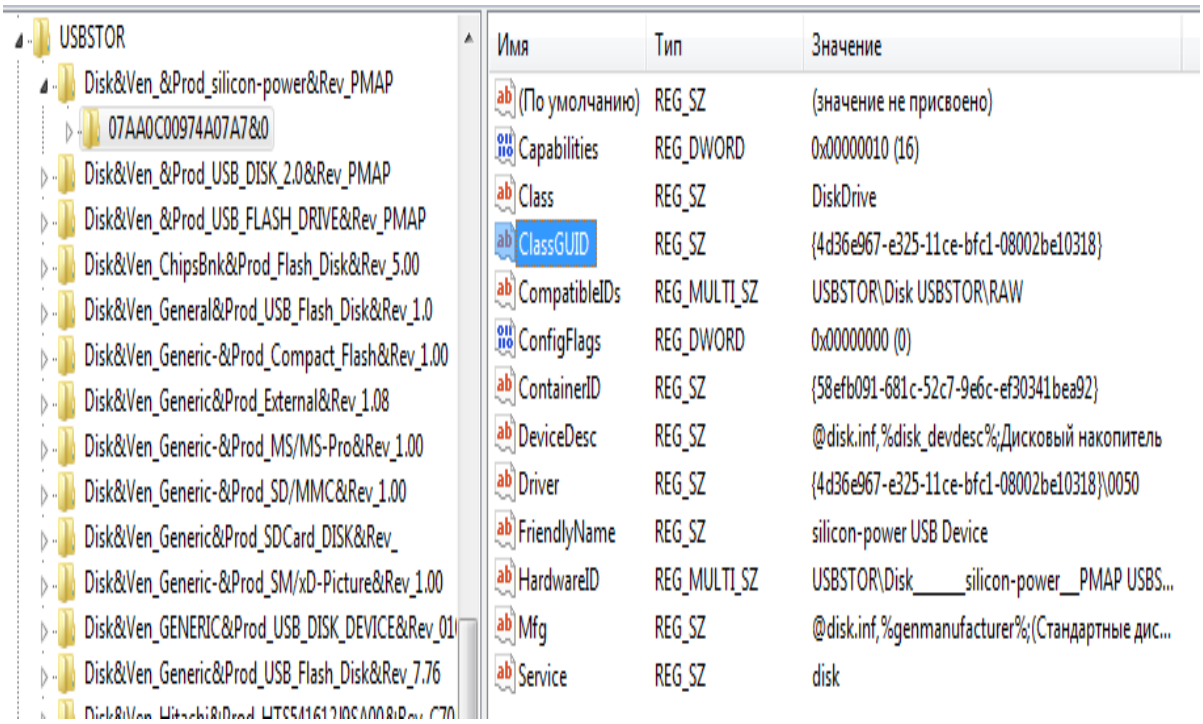


Рис. 44. Данные из реестра о подключении внешних устройств.

Используя данные из файла: «setupapi.log» для WindowXPи данные из файла «setupapi.dev.log» для Window 7, по серийному номеру устройства можно определить дату и время его подключения. Для чего необходимо:

- открыть файл для просмотра;
- определить с помощью поиска строку, содержащую серийный номер устройства или GUID;
- выше в скобках будет указана дата и время подключения.

Важно отметить, что данная информация изменяется через определенное время и не может мгновенно отразить данные о подключении устройств.

Поиском строк «#I121 Установка устройства» в файле «setupapi.log»можно определить даты подключаемых ранее устройств.

Пример фрагмента файла «setupapi.log»для XP

#I121 Установка устройства "STORAGE\REMOVABLEMEDIA\7&BD57F20&0&RM" успешно завершена.

[2010/10/24 21:19:31 2456.241 DriverInstall]

Данные о подключенных устройствах отражаются в журнале событий, в частности в меню «приложение» и «система».

Для меню «Система» win7 код событий где можно посмотреть информацию о подключённых внешних устройствах «20001», «10000», «20003». Данные коды событий можно задать в «фильтре» программы просмотра журналов

Ниже на рисунке 45 приведено изображение окна программы с выборкой фильтра «10000».

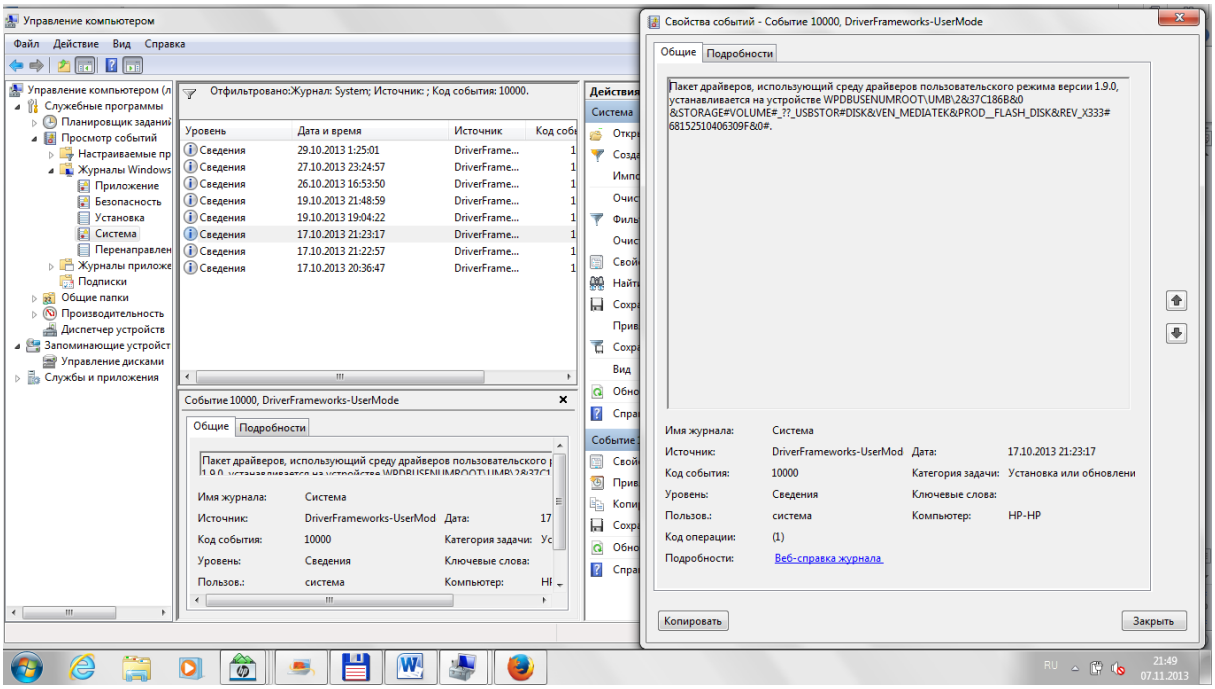


Рис. 45. Окно программы с выборкой фильтра «10000».

Для просмотра файлов журналов событий можно использовать штатные средства операционной системы, в меню «действия» программного обеспечения «управление компьютером» открыв исследуемый файл. Или воспользоваться специализированным программным обеспечением, например «Event Log Explorer».

Данные об установленном программном обеспечении MicrosoftOffice хранятся в ветвях реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\ (далее запись типа: 9140110900063D11C8EF10054038389C)\InstallProperties

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\ XX.0\Registration\ (далее запись типа: {90110419-6000-11D3-8CFE-0150048383C9})

Для Windows 7

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\XX.0\Registration\ (далее запись типа: {90120000-0016-0000-0000-0000000FF1CE})

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Installer\UserData\S-1-5-18\Products\ (далее запись типа: 00002109610000000000000000F01FEC)\InstallProperties

Для WindowsXP.

где XX.0 код программного обеспечения MicrosoftOffice.

Для определения проведенных действий операционной системой семейства "Windows" производится просмотр журналов событий операционной системы.

В "WindowsXP" данные файлы по умолчанию расположены в директории "%SYSTEMROOT%\system32\config\ и имеют расширение ".Evt"

Для Windows 7 данные файлы по умолчанию расположены в директории "%SYSTEMROOT%\System32\Winevt\Logs\" и имеют расширение ".Evtx".

Просмотром данного журнала возможно определить:

- временные рамки работы операционной системы;
- временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале событий операционной системы "Windows";
- временные рамки подключения - отключения сетевых ресурсов (сетевого адаптера) запуск которых отображается в журнале событий операционной системы "Windows", и ряд других параметров.

К программным продуктам, которые оставляют различные следы при работе в операционных системах относятся:

1) Браузеры (Internet Explorer, Opera, Mozila Firefox, Google Chrome идр.);
2) Программы для переписки (ICQ, QIP, Skype и д.р.);
3) Программы – почты (Outlook Express, The Bat);
4) Другие программы – игры, торенты и т.д.

При работе в браузерах следы остаются в файлах cookies, cache браузера и реестре.

Cookies ("куки") – это текстовые файлы содержащие информацию о работе браузера, в том числе данные о посещении ресурсов и хэши паролей обращения к сетевым ресурсам.

Для WindowsXP файлы Cookies хранятся в следующих местах.

Cookies в Internet Explorer: %SYSTEMDRIVE%:\Documents and Settings\[имя пользователя]\Cookies\, а так же

%SYSTEMDRIVE%:\Documents and Settings\[имя пользователя]\Local Settings\Temporary Internet Files\;

Cookies в Opera: %SYSTEMDRIVE%:\Documents And Settings\[имя пользователя]\Local Settings\Application Data\Opera

Cookies в Mozila Firefox: %SYSTEMDRIVE%:\Documents and Settings\[имя пользователя]\Application Data\Mozilla\Firefox\Profiles

Cookies в Google Chrome: %SYSTEMDRIVE%:\Documents and Settings\[имя пользователя]\Local Settings\Application Data\Google\Chrome\ User Data\Default

В windows XP, кэш Opera находитсяв%SYSTEMDRIVE%:\ Documents and Settings\[имя пользователя]\ AppData\Local Settings\Opera\Opera [версия]\cache

В windows 7 и выше, кэш Opera находится в %SYSTEMDRIVE%:\ Users \[имя пользователя]\ AppData\Local\Opera\Opera [версия]\cache

Кэш Firefox находится по адресу: %SYSTEMDRIVE%:\ Documents and Settings\[имя пользователя]\AppData\Local\Mozilla\Firefox\Profiles\ [случайный номер профиля].default\cache

В windows 7 и выше %SYSTEMDRIVE%:\ Users \[имя пользователя] \AppData\Local\Mozilla\Firefox\Profiles\[случайныйномерпрофиля].Default\ cache

Кэш Google ChromeB windows XP находится по адресу: %SYSTEMDRIVE%:\Documents and Settings \[имя пользователя]\AppData\ Local\Google\Chrome\User Data\Default\Cache

В windows 7 Кэш Google Chrome находится по адресу: %SYSTEMDRIVE%:\Users\[имя пользователя]\AppData\Local\Google\ Chrome\User Data\Default\Cache

Кэш Internet ExplorerB windows XP находится по адресу: %SYSTEMDRIVE%:\Documents and Settings \[имя пользователя]\Local Settings\Temporary Internet File.

В windows 7 Кэш Internet Explorer находится по следующему адресу: %SYSTEMDRIVE%:\Users\[имя пользователя]\Local Settings\Temporary Internet File.

Данные из реестра операционных систем содержащих с ведения об интернет браузерах.

Ветвь реестра браузера Internet Explorer: HKEY_CURRENT_USER\ Software\Microsoft\Internet Explorer;

Ветвь реестра браузера Opera: HKEY_LOCAL_MACHINE \ Software \ Opera;

Ветвь реестра браузера Mozila Firefox: HKEY_LOCAL_MACHINE \ Software \Mozilla\Mozilla Firefox;

Ветвь реестра браузера Google Chrome: HKEY_LOCAL_MACHINE \ Software \Google Chrome;

Данные об электронных пейджинговых сообщениях и электронных почтовых сообщениях.

Историю сообщений для ICQ можно посмотреть по следующему адресу: %SYSTEMDRIVE%:\Documents and Settings\Имя пользователя\ ApplicationData\ICQ\ (для WindowsXP);

%SYSTEMDRIVE%:\Users\Имя пользователя\Application Data\ICQ\ (для Windows 7 и выше)

Для QIP: %SYSTEMDRIVE%:\Program Files\QIP\Users\<номер UIN>\History\

QIP Infium: %SYSTEMDRIVE%:\Documents and Settings\<имя пользователя>\Application Data\QIP\Profiles\<номер UIN>\History\ (для Windows XP);

%SYSTEMDRIVE%: \Users\<имя пользователя>\Application Data\QIP\Profiles\<номер UIN>\History (для Windows 7 и выше).

История сообщений Skypex ранится по адресу: %SYSTEMDRIVE%:/ Documents and Settings/Имя_Пользователя/ApplicationData/Skype (для Windows XP);

%SYSTEMDRIVE%:/users/Имя_Пользователя/Application Data/Skype (для Windows 7 и выше).

MicrosoftOutlookExpress в Windows XP сохраняет файлы почтовых сообщений с расширением DBX по адресу: %SYSTEMDRIVE%:\Documents and Settings\имя пользователя\LocalSettings\ ApplicationData\Identities\[indentity number]\Microsoft\OutlookExpress\, где[indentity number] – некоторый идентификационный номер.

В Windows 7 и выше: %SYSTEMDRIVE%:\Users\имя пользователя Settings\Application Data\Identities\indentity number\Microsoft\Outlook Express\

Просмотров ветви реестра HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Explorer\FileExts можно определить данные об открытых файлах из проводника windows

Ниже приведены данные о служебных файлах браузера Firefox содержащих криминалистически значимую информацию.

Закладки и история просмотра содержатся в файле: places.sqliteЭтот файл содержит все закладки и список посещенных сайтов «ЖУРНАЛ».

В файле key3.db хранится база данных ключей для паролей

Сохраненные пароли находятся файлы signons.sqlite.

В файле permissions.sqlite содержатся данные о настройках и разрешениях доступа к сайтам.

В файле formhistory.sqlite содержатся данные набранные в поисковой строке.

В файле cookies.sqlite содержатся данные «Cookies».

В файле mimeTypes.rdf содержатся данные о действиях «по умолчанию» с известными типами файлов.

В файле downloads.sqlite хранится информация о скачанных файлах.

Проведение специальных мероприятий в отношении мобильных телефонов.

Развитие современных средств передачи и обработки данных предусматривает наличие оперативного доступа к информации, обрабатываемой в системе ИСОТ. Качественно реализовать доступ к данной информации возможно только с использование мобильных устройств под управлением ОС «Android», остальные системы «WiwdowsPhon» и «IOS» не обеспечивают требуемого уровня защиты информации от иностранных разведок. Но системы под управлением «Android» имею ряд недостатков связанных с особенностями функционирования операционной системы. В этой связи необходимо сделать ряд важных замечаний.

При проведении исследования мобильных телефонов под управлением ОС Android используют статический и динамический анализ. Исследование проводится на физическом дампе памяти мобильного устройства. Не допус-

кается установка антивирусного программного обеспечения, с целью выявления вредоносного программного обеспечения, на исследуемый мобильный телефон! Большинство приложений, работающих в ОС Android, используется язык программирования Java. Выполняются программы в системе посредством регистровых виртуальных машин Dalvik до версии 4.4 и Android Runtime или ART, начиная с версии 4.4, имеется выбор виртуальной машины.

Приложения для ОС Android являются исполняемыми приложениями формата apk, указанный файл представляет собой ZIP-архив, включающий байт-коды, ресурсы, сертификаты и manifest-файл. С криминалистической точки зрения реализация незаконного перевода денежных средств, с помощью специализированного программного обеспечения (вредоносного) осуществляется после установки apk-файлов в соответствующие места файловой системы Android, для системных приложений это обычно /system/app, для пользовательских – /data/app. Наличие программ детектируемых антивирусным программным обеспечением как вредоносные, не подтверждает реализацию функций данных программ, эти программы могут находиться в памяти мобильного телефона, но быть активированными. Лишь выявление соответствующего (вредоносного) кода в системных /system/app или пользовательских /data/app областях памяти свидетельствует об активации этого программного обеспечения.

Для проведения исследования необходимо выполнить следующие действия:

- получить физический дамп памяти мобильного телефона (посекторная бинарная копия), для чего можно использовать как криминалистические средства «XRY», «UFED», «МОБИЛЬНЫЙ КРИМИНАЛИСТ», так и программное обеспечение, предназначенное для работы с телефонами под управлением ОС Android, например «Android Debug Bridge (ADB)»;

- из полученного дампа памяти, с помощью программ восстановления данных поддерживающих работу с посекторными копиями, восстанавливается удаленная информация, (для восстановления можно использовать «R-studio», «UFS Explorer», или криминалистическое программное обеспечение «Belkasoft», «AccessData»);

- выявить файлы, в том числе и восстановленные после удаления, с расширением apk, расположенные в системных /system/app или пользовательских /data/app областях памяти мобильного телефона;

- получить с помощью специализированного программного обеспечения содержание файлов с расширением apk (т.е. провести декомпиляцию);

- проанализировать данные содержащиеся в файле «AndroidManifest.xml»;

- произвести статический анализ apk-файлов, в том числе восстановленных после удаления, с помощью антивирусного программного обеспечения, в случае использования ресурса VirusTotal возможно получит более полную информацию, в том числе о ресурсах к которым обращается исследуемое программное обеспечения (в случае если оно определяется как вредоносное);

- произвести динамический анализ apk-файлов, в том числе восстановленных после удаления, для проведения динамического экспресс анализа можно использовать интернет ресурс https://anubis.iseclab.org/, виртуальные машины и программное обеспечение «Android SDK» или программный продукт DroidBox [указанный программный продукт позволяет собрать следующую информацию о программе и ее деятельности в системе:

- хеш-сумма APK-файла (алгоритмы MD5, SHA-1 и SHA-256);
- сведения о полученных и отправленных по сети данных;
- сведения об операциях чтения и записи файлов;
- сведения о запущенных службах и загруженных классах;
- сведения о сборе и отправке пользовательских данных;
- сведения о разрешениях, которые получило приложение;
- сведения о криптографических операциях, осуществляемых приложением с использованием Android API;
- сведения об отправляемых SMS-сообщениях и осуществляемых вызовах.

По результатам будет сформирован набор файлов в формате JSON, содержащих указанные сведения.

Необходимо отметить, что рассматриваемый программный продукт предназначен для работы в операционных системах Linux и Mac OS X, но для его использования можно использовать виртуальные машины;

- произвести поиск данных, в том числе и удаленных по заданным критериям (исходя из информации предоставленной инициатором исследования и информации полученной в ходе статического и динамического анализа apk-файлов);
- выявить приложений содержащие максимальные приоритет выполнения «android:priority=», Минимальный приоритет выполнения равен «-1000», максимальный равен «1000» (осуществляется поиском);
- выявить приложения содержащие разрешения на отправку и получение и скрытие от пользователя SMS-сообщений («android.permission.SEND_SMS», «android.permission. RECEIVE_SMS» и «BlockAllSms»;
- произвести сравнение дат создания файлов и директорий в служебной области, как правило все файлы в служебной области имеют одно врем создания, наличие файлов с различающимися датами может свидетельствовать о создании данных файлов с правами супер администратора ROOT или использования команды системного администрирования SUDO;
- по параметрам, (хэшсумма, размер, наименование), выявленных apk-файлов произвести поиск данных в памяти мобильного телефона, особое внимание обратить на системную область, выделенную для сохранения данных. В случае обнаружения аналогичных файлов в данном месте, а так же соответствующей информации об установке или сохранении данных файлов содержащиеся в файлах интернет браузерв, можно сделать предположение о способе проникновения кода в ОС.

При извлечении информации из файлов с расширением apk необходимо пользоваться специализированным программным обеспечением. При непосредственном извлечении информации из файлов как из архивов или использовании некоторых интернет ресурсов предназначенных для извлечения содержимого файлов наблюдаются потери данных и искажение содержимого. Для извлечения и исследования программного кода содержащегося в файлах с расширением apk, оптимально использование следующего программного обеспечения программного обеспечения «ApkTool» , «Dex2Jar» и «JD-GUI8»!

ApkTool позволяет произвести извлечение данных из apk-файлов. В результате будут сформированы директория с именем аналогичным имени apk-файла. В данной директории в основном содержатся следующие данные:

- файл Android Manifest, содержит сведения о разрешениях, запрашиваемых приложением, о точках входа, а также список активности приложения, служб и методов передачи информации;

- файл classes.dex, является исполнительной частью приложения, и содержит все его скомпилированные классы, представленные в виде байт-кодов. Необходимо отметить, что байт-код здесь преобразован в инструкции для виртуальной машины Android, так как последняя, в отличие от виртуальной машины Java, основана на регистрах.

- каталог res, содержит XML-файлы, описывающие макет приложения, а также необходимые ему графические файлы и т.д.;

- каталог META-INF, содержит контрольные суммы файлов входящих в состав apk-файла, данные сигнатур можно использовать для быстрой идентификации в памяти исследуемого устройства программного обеспечения.

Dex2Jar позволяет преобразовать файлы с classes.dex (байт-код) в classes.dex.dex2jar.jar (java-код). Анализ полученного файла, содержащего исходный код Java, может быть произведен посредством программного продукта JD-GUI.

Список литературы.

1. Программно-аппаратный комплекс поиска побочных электромагнитных излучений и наводок "Навигатор", Описание применения.
2. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
3. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации / Хореев А.А. – М.: НЦП «Аналитика», 2008. – 436 с.
4. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 4-е издание, стереотип / Малюк А.А., Пазизин С.В., Погожин Н.С. – М.: Горячая линия-Телеком, 2011. – 146 с.
5. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: В 2 частях. Часть 2. Практические аспекты комплексного технического контроля эффективности мер безопасности систем управления в органах внутренних дел. Учебное пособие / Чекалин А.А. – М.: Горячая линия-Телеком, 2006. – 232 с.
6. Баркалов Ю.М. Подготовка экспертов по производству компьютерных судебных экспертиз [Текст] : методические рекомендации. Электронное издание, регистрационный номер – 0321304879, ВИ МВД России, 2014. – 65 с.
7. Бабкин А.Н., Киселев В.В., Лунев Ю.С., Баркалов Ю.М.. Поиск и восстановление информации в операционной системе MAC OS X при производстве компьютерных экспертиз: методические рекомендации [Текст] : ВИ МВД России, 2015 – 31с.