передавать информацию по радиоканалу, сложностью определения злоумышленника (для закладных устройств).

Также злоумышленник может получать информацию следующими способами:

— наблюдение из окна противоположного здания текста и изображений на плакатах, экранах, укрепленных на стенах кабинета;

— подслушивание разговора в кабинете через приоткрытую дверь в приемную руководителя;

— наблюдение через окно противоположного здания за участниками совещания;

— наблюдение через приоткрытую дверь за участниками совещания;

— перехват побочных электромагнитных излучений радиоэлектронных средств и электрических приборов, размещенных и работающих в кабинете во время разговора;

— перехват опасных сигналов, содержащих речевую информацию, распространяющихся по проводам телефонных линий связи, пожарной сигнализации, электропитания и заземления;

— подслушивание речевой информации акустических сигналов, распространяющихся по воздуховодам и трубам отопления;

— скрытое проникновение к источникам информации, хранящихся в ящиках стола, в компьютере, в сейфе.

Внедрение системы защиты информации позволяет предотвратить или снизить величину ущерба, наносимого владельцу системы, вследствие реализации угроз безопасности информации. При её создании необходимо защищать информацию во всех фазах существования и от любых несанкционированных действий.

Выбор конкретных технических средств защиты информации осуществлялся комплексным методом определения уровня качества изделия. Для определения комплексных показателей качества необходимо было выполнить следующее: провести преобразование параметров, выраженных несколькими числовыми значениями в параметры, выраженные одним числовым значением; провести нормирование значений параметров; назначить параметрам коэффициенты значимости; провести нормирование значений коэффициентов значимости; провести расчет комплексных показателей качества; провести анализ и оценку полученных результатов. Далее производились расчеты (количества виброизлучателей, электромагнитной совместимости технических устройств, потребляемой мощности) для правильной расстановки выбранных технических изделий в защищаемом помещении.

В результате была разработана система защиты кабинета директора, которая позволяет предотвратить утечку информации или снизить величину ущерба, вследствие реализации угроз безопасности информации.

Список использованных источников:

1.Торокин, А. А. Инженерно-техническая защита информации : учеб. пособие / А. А. Торокин. — М. : Гелиос АРВ, 2005. — 960с.

2.Бузов, Г.А. Защита информации от утечки по техническим каналам : Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. — М. : Горячая линия — Телеком, 2005. — 416 с.

# СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ КОМПАНИИ ПО РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Белич А. А.*

*Дусь А.В. – ассистент*

Вопросы информационной безопасности занимают особое место и в связи с возрастающей ролью в жизни общества требуют к себе все большего внимания. Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация.

Для успешной работы многих компаний, особенно занимающихся разработкой программного обеспечения, чрезвычайно важно поддерживать безопасность и целостность своей компьютерной сети. Это обязывает многие компании к организации индивидуальной системы защиты информации локальной вычислительной сети.

Система защиты информации ЛВС включает в себя совокупность различных средств и методов, направленных на предотвращение утечки информации по различным каналам.

Стандартная система защиты ЛВС производится по следующим направлениям:

Аппаратные средства защиты информации

Рассматриваются различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др.

Вторую – генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, "перекрывающих" потенциальные каналы утечки информации или позволяющих их обнаружить.

Технические методы и средства комплексной защиты.

Изучаются технические методы и средства защиты информации в ЛВС и проводится их сравнительный анализ. Описываются, такие методы, как криптографическая защита информации, идентификация, аутентификация и управление доступом, обеспечение безопасности операционных систем, технологии межсетевого экранирования и системы обнаружения компьютерных атак, технологии защиты от вредоносных программ и спама, управление информационной безопасностью, технологии обнаружения и предотвращения вторжений, применение виртуальных частных сетей.

Организационные методы комплексной защиты локальной сети.

Рассматриваются организационные мероприятия по комплексной защите сети, изучается порядок аттестации объектов информатизации, имеющих в своем составе ЛВС, а также формы и содержание выдаваемых документов по аттестации. Описываются вопросы администрирования и контроля безопасности информации в ЛВС, организации документооборота и обеспечения режима конфиденциальности при работе с документами; корректируются основные должностные обязанности администратора безопасности, операторов рабочих станций компьютерной сети.

Организация системы защиты локальной вычислительной сети происходит с использованием описанных методов и средств, учитывая индивидуальные характеристики корпоративной сети: используемое оборудование, программное обеспечение, коммуникации, количество сотрудников компании, вид занимаемых помещений и прилегающей территории.

Грамотно составленная система защиты информации локальной компьютерной сети предприятия существенно повысит безопасность и качество выполняемой работы.

Список использованных источников:

1.Биячуев, Т.А. Безопасность корпоративных сетей. – СПб: ГУ ИТМО, 2004. – 20 с.

2.Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – Москва: ДМК Пресс, 2012. – 30 с.

# ИССЛЕДОВАНИЕ ДЕГРАДАЦИИ ФУНКЦИОНАЛЬНЫХ ПАРАМЕТРОВ ИЗДЕЛИЙ ЭЛЕКТРОННОЙ ТЕХНИКИ ПО РЕЗУЛЬТАТАМ УСКОРЕННЫХ ИСПЫТАНИЙ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Янцевич Ю. В.*

*Боровиков С. М. – канд. техн. наук, доцент*

Для биполярных транзисторов (БТ) серийного производства с отработанной технологией были поставлены задачи по исследованию закономерностей дрейфа функциональных параметров при длительной наработке транзисторов. С целью сокращения продолжительности испытаний на длительную наработку принято решение о проведении ускоренных испытаний, выполняемых по типовым методикам. Важным фактором в оценке работоспособности приборов является прогнозирование надежности.

Во время проведения экспериментальных исследований выборки БТ на длительную наработку выполнялось измерение функциональных параметров. Испытание приборов на долговечность производилось в схеме с общей базой. Использовалась схема испытаний, приведенная на рис. 1.

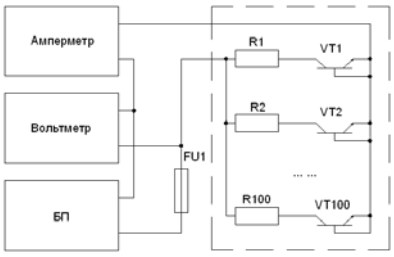


Рис. 1

В докладе приведены результаты ускоренных испытаний на длительную наработку. Установлено [1], что комбинация высокой температуры и обратного смещения на коллекторном переходе является наиболее оптимальной при ускоренных испытаниях БТ на длительную наработку. При реализации испытаний по данной методике использована эта комбинация нагрузок. Выбран режим и рассчитано время проведения ускоренных испытаний. С использованием данных результатов получены деградационные математические модели функциональных параметров $U_{КЭнас}$ и $h_{21Э}$. Использовался метод наименьших квадратов [2].