Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное профессиональное
образовательное учреждение
«Белгородский индустриальный колледж»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ ПМ 03.
Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

ДЛЯ СПЕЦИАЛЬНОСТИ
11.02.10 Радиосвязь, радиовещание, телевидение
(углубленной подготовки)

Разработал: Рачинский С.А.
Рассмотрено и одобрено ЦК
«Радиовещание и
системы диспетчерского
управления»
Протокол заседания № 1
от 30 августа 2019г.
Председатель ЦК
_____Чобану Л.А

Белгород 2019г.

Рачинский Сергей Андреевич

СОДЕРЖАНИЕ

МДК 03.01. Технология применения комплексной защиты информации в системах радиосвязи и сетях вещания

Тема 1.2. Методы и способы защиты информации		
№ Л/Р	**Тема лабораторной работы**	**Кол-во часов**
	МДК 03.01	
1-2	Обнаружение скрытого видеонаблюдения	**4**
3-4	Ознакомление с многофункциональным имитатором сигналов «Шиповник 2»	**4**
5-6	Работа с устройствами комбинированной защиты объектов информатизации	**4**
7-8	Аттестации помещения по требованиям безопасности информации	**4**
9-10	Технические средства защиты информации в телефонных линиях	**4**
11-12	Поиск и измерение побочных электромагнитных излучений и наводок	**4**
13-14	Генераторы псевдослучайных последовательностей.	**4**
15-16	Линейный конгруэнтный и рекуррентный генераторы ПСП.	**4**
17-18	Контроль эффективности защиты речевой информации	**4**
19-20	Исследование принципов формирования псевдослучайных последовательностей и методов их тестирования	**4**
21-22	Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств	**4**
23-24	Поиск каналов утечки речевой информации	**4**
25-26	Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.	**4**
27-28	Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем охранной (пожарной) сигнализации	**4**
29-30	Исследование принципов построения симметричных криптосистем и их использования для защиты данных	**4**
31-32	Исследование процедуры формирования и проверки электронной цифровой подписи на основе ассиметричного алгоритма RSA	**4**
33-34	Исследование схемы разделения секрета	**4**
35-36	Изучение средств выявления каналов утечки информации на примере высокочувствительного сканирующего приемника AR-5000A «КВАДРАТ»	**4**
37	Обнаружение приборов наблюдения и оптических приборов	**2**
	МДК 03.02	
1	Обнаружение приборов наблюдения и оптических приборов	**2**
2-4	Поиск каналов утечки информации с помощью нелинейного локатора. Поиск и обнаружение радиозакладок в помещении	**6**
5-7	Поиск каналов утечки информации с помощью индикатора поля. Поиск и обнаружение радиозакладок в помещении	**6**
8-10	Изучение средств выявления каналов утечки информации на примере программно-аппаратного комплекса измерения ПЭМИН «СИГУРД»»	**6**
11-12	Взлом моноалфавитного подстановочного шифра методом частотной атаки	**4**
13-14	Одноразовые блокноты	**4**
15-16	Сеть Фейштеля	**4**
17-18	Шифрование с открытым ключом и электронная цифровая подпись на GPG	**4**
19-20	Метод шифрования с открытым ключом RSA	**4**

21-22	Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.	**4**
23-25	Исследование основных характеристик сигналов на основе использования аппаратно-программного комплекса радиоконтроля «КВАДРАТ»	**6**
26-28	Скрытая передача информации в JPEG изображениях	**6**
29-31	Запись и чтение информации для пластиковых карт с магнитной полосой	**6**
32-35	Виды штрих-кодов, их генерация и считывание	**6**

Лабораторная работа №1-2

«Обнаружение скрытого видеонаблюдения»

Цель работы: Ознакомиться с различными способами обнаружения скрытых видеокамер;
Порядок выполнения работы

1. Теоретическая часть

1А.Обнаружители видеокамер.

Как известно, на каждое действие найдется противодействие. Стоит только появиться новому «жучку», специалисты начинают работу по созданию средств его поиска и нейтрализации. С течением времени устройства защиты развиваются, совершенствуются, приобретая все больше полезных функций и становясь все более удобными в использовании. Аналогичные процессы происходили и с устройствами обнаружения скрытых видеокамер.

Различные виды подглядывания (скрытая фото- и видеосъемка, использование средств ночного видения и т. п.) всегда привлекали шпионов; немало усилий было потрачено злоумышленниками на их создание и совершенствование. Размеры видеокамер с течением времени становились все меньше и меньше, а характеристики получаемого изображения улучшались.

Появились проводные и беспроводные видеокамеры, камеры, передающие изображение по радиоканалу, и камеры, включаемые дистанционно - по потребностям злоумышленника. В результате всех трудов сегодня скрытую видеокамеру можно незаметно установить буквально куда угодно: в мебель, стены, предмет одежды - все зависит от фантазии злоумышленника - и вести съемку практически незаметно для человека.

Обнаружить эти многочисленные видеокамеры можно несколькими известными на сегодняшний день способами:

- с помощью индикатора поля (в случае если передача информации с камеры ведется по радиоканалу);
- оптическим способом (лазерный луч, посылаемый с оптического обнаружителя, отражается от объектива видеокамеры);
- электромагнитным обнаружителем видеокамер.

Приборы первого типа довольно широко распространены на Западе, однако они представляют собой обычные индикаторы поля, поэтому остановимся более подробно на двух последних.

Оптические обнаружители работают на основе эффекта световозвращения. Описать этот эффект можно следующим образом. Поскольку все оптические приборы наблюдения (в нашем случае речь идет о камерах) содержат светочувствительный элемент (например, ПЗС-матрицу), луч, направленный на этот элемент, отразится от него и вернется обратно к источнику, т. е. к обнаружителю. Таким образом, оператор посылает зондирующий луч на место предполагаемого размещения скрытой видеокамеры, и в случае, если камера действительно установлена, он увидит блик, отраженный от светочувствительного элемента.

Однако помимо нужного сигнала в поле зрения будут попадать излучения от других элементов, для избавления от них в оптические обнаружители включена система отсеивания таких шумов. В некоторых приборах для этого используется ИК-пропускающий фильтр. При этом параметры лазерного луча (или светодиодной подсветки) также играют большую роль при обнаружении, при производстве они тщательно подбираются опытным путем.

У такого принципа работы есть свои преимущества и недостатки: с одной стороны, он позволяет обнаруживать оптические устройства различного типа (от снайперских винтовок до биноклей), а с другой - уже придуманы средства противодействия оптическим обнаружителям - специальные светофильтры для отсеивания световых волн, имеющих определенную длину.

Существует еще один способ выявления видеокамер - с помощью электромагнитных обнаружителей. Для понимания принципа работы таких приборов нужно сказать несколько слов о строении скрытых видеокамер. Как уже было замечено ранее, в подавляющем большинстве современных скрытых видеокамер в качестве фотоприемника (устройство для трансформации светового сигнала в электрический) используется ПЗС-матрица (прибор с зарядовой связью).

Она обслуживается процессором, т. е. считывателем сигнала, который потом формирует видеосигнал. В составе процессора имеется осциллятор, который излучает на какой-то фиксированной частоте. Сам по себе осциллятор на определенной частоте излучает на небольшое расстояние, однако он имеет побочные излучения, складывающиеся из гармоник основной частоты.

Эти гармоники кратны основной частоте и также излучают на небольшие расстояния (чем выше гармоника, тем меньше расстояние), однако среди них есть гармоники, которые очень хорошо проникают сквозь корпус видеокамеры. Камера определенного типа хорошо излучает на определенных гармониках, это обычно определяется опытным путём, и затем полученный образ излучения записывается в память обнаружителя видеокамер. Количество записанных в память гармоник для каждого типа камер может быть различным.

Собственно же обнаружение происходит следующим образом. Прибор обследует электромагнитную обстановку в помещении, обнаруживает какие-то частоты и сравнивает их с образами, занесенными в память. Поскольку частота осциллятора камеры находится в некотором промежутке спектра, обнаружитель в режиме поиска разбивает полосу спектра на отдельные небольшие кусочки, в которых проводит более детальное обследование, постепенно повышая чувствительность.

Далее обнаружитель должен принять решение, является ли частота частотой процессора видеокамеры или это случайная помеха. Для отсечения случайных помех может, например, применяться двойной цикл верификации и подтверждения, а в некоторых приборах каждый подозрительный участок спектра обследуется 4 раза, и только после этого пользователю выдается окончательное решение о принадлежности частоты осциллятору видеокамеры.

На сегодняшний день на рынке существует немало видеокамер различных типов, однако в России в большинстве своем используются видеокамеры типа PAL, реже NTSC; есть и другие типы, но они редко встречаются на практике. Производители по-разному решали проблему систематизации образов камер в памяти прибора. Например, в прибор заложена возможность регистрации и запоминания образов камер, найденных в процессе поиска, чтобы в последующем использовать эти данные. В других приборах эти данные сбрасываются.

Связано это со следующим: как уже было сказано ранее, частота осциллятора может изменяться в зависимости, как от температуры окружающей среды, так и электронных компонентов самой камеры. Скрытые камеры, работающие не от сети, чаще всего включаются злоумышленниками дистанционно для экономии заряда, а при включении камера начинает медленно нагреваться, ее частота меняется, соответственно, в ранее найденном участке спектра камера уже не излучает. Таким образом, теряется смысл запоминания такого образа, потому что через некоторое время камера может пропасть, и этот участок будет исследоваться зря.

Для локализации местонахождения камеры пользуются отображением уровня излучения на экране обнаружителя, причем в одних приборах на дисплее виден интегральный уровень излучения, в других отображается уровень самой большой гармоники. Следует сказать, что последний вариант предпочтительнее, так как нередко одна из гармоник, из которых складывается интегральный уровень, может пропасть, т. е. оказаться в так называемой мертвой зоне.

Происходит это из-за того, что излучения вследствие интерференции наложения волн и отражения от поверхностей могут увеличиваться, а могут и полностью пропадать, что приведет к значительному изменению интегрального уровня, а значит, к принятию неправильного решения, что в той стороне камеры нет. Дальность обнаружения скрытых видеокамер и для оптических, и для электромагнитных обнаружителей колеблется в пределах нескольких метров. В первом случае на дальность влияют несколько факторов: тип подсветки (импульсная или непрерывная, в некоторых приборах реализована возможность выбора), наличие или отсутствие подстройки по диоптриям, острота зрения оператора, освещенность помещения, в котором проводится обзор, и др.

1.2. Дальность обнаружения скрытых видеокамер

Дальность обнаружения скрытых видеокамер и для оптических, и для электромагнитных обнаружителей колеблется в пределах нескольких метров.

Для оптических обнаружителей на дальность влияют несколько факторов: тип подсветки (импульсная или непрерывная, в некоторых приборах реализована возможность выбора), наличие или отсутствие подстройки по диоптриям, острота зрения оператора, освещенность помещения, в котором проводится обзор.

Дальность действия электромагнитных обнаружителей зависит в основном от типа скрытых видеокамер и от того, как скрытая видеокамера излучает.

Плохо излучающие скрытые видеокамеры обычно находятся с расстояния около 3 м, а хорошо излучающие - вплоть до 50 м, средняя дальность обнаружения составляет 7-10 м. Данные параметры и характеристики одинаковы для всех электромагнитных обнаружителей скрытых видеокамер.

1.3. Время и условия обнаружения (поиска) скрытых видеокамер

Время поиска для электромагнитных обнаружителей в большей степени зависит от количества типов видеокамер, внесенных в память обнаружителя. Современные электромагнитные обнаружители способны вести поиск видеокамер практически незаметно для окружающих (в большинстве из них существует световая, звуковая и вибрационная индикация).

Есть приборы, оснащенные антенной скрытого ношения, что позволяет вести поиск максимально незаметно (однако, прилегание антенны прибора к телу человека достаточно сильно снижает ее чувствительность, поиск удобнее проводить, держа обнаружитель в вытянутой руке в открытом пространстве).

В некоторых моделях обнаружителей предусмотрена возможность постоянного мониторинга помещения и отправки в случае обнаружения данных о подозрительном сигнале на удаленную ПЭВМ или обмена информацией с ПК через mini USB-порт, что позволяет загружать обновления базы данных и программного обеспечения.

1.4. Особенности обнаружителей разных принципов действия.

Оптические же обнаружители неспособны вести скрытый поиск, и это может послужить серьезным аргументом в пользу приборов электромагнитного типа. Человек, осматривающий помещение при помощи оптического обнаружителя, точно не останется незамеченным, что во многих случаях может быть нежелательным. Еще следует отметить, что поиск с использованием оптических обнаружителей требует времени, а также терпения и предельной внимательности оператора. Однако оптические обнаружители, в отличие от электромагнитных, способны выявлять все виды видеокамер в независимости от того, выключены они или включены. В заключение хотелось бы сказать, что при выборе типа обнаружителя необходимо отталкиваться от задачи, которую требуется выполнять: в ситуации, когда быстрота и скрытность поиска не играют принципиальной роли, можно применять оптические обнаружители, цена которых как минимум в два раза ниже, чем стоимость приборов электромагнитного типа.

1.5. Оптико-электронный прибор для дистанционного обнаружения систем скрытого видеонаблюдения "АНТИСВИД"

Назначение: для обнаружения миниатюрных систем скрытого видеонаблюдения, замаскированных в деталях интерьера, помещений, одежде, личных вещах и т.п.

Принцип действия прибора основан на использовании физического явления световозвращения, возникающего при дистанционном зондировании лазерным пучком поля обзора с последующей регистрацией ретроотраженного излучения инспектируемой системой скрытого видеонаблюдения и индикацией ее положения на экране монитора в виде яркого блика.

Преимущества: расширение рабочего диапазона по дальности в область малых значений от 0 до 1...3 метров за счет оригинальной схемы построения прибора. Энергетика прибора обеспечивает высокую вероятность обнаружения систем скрытого видеонаблюдения в условиях высоких уровней естественных фонов.

Технические характеристики

Дальность действия, м	0.15
Диаметр объектива системы скрытого видеонаблюдения, мм, min	1
Диапазон уровней естественной фоновой освещенности, лк, до	1000
Спектральный диапазон работы прибора	ближний инфракрасный
Углы обзора, град	360 - (60..+60)
Потребляемая мощность, Вт	5

1.6. Профессиональный обнаружитель скрытых видеокамер "Оптик-2"

Устройство "Оптик-2" предназначено для поиска и локализации скрытых, камуфлированных в интерьере видеокамер (в том числе с объективом типа «pinhole») независимо от их состояния и типа передачи или записи видеосигнала.

Способ обнаружения, реализованный в "Оптике-2", основан на оптической локации и позволяет обнаружить объектив видеокамеры за счёт эффекта световозвращения или "обратного блика". При обнаружении объектива скрытой камеры в объективе «Оптика-2» будет наблюдаться точечное пятно зелёного или красного цвета - результат отражения.

Конструктивные особенности: выполнен в виде бинокля в обрезиненном металлическом корпусе.

Технические преимущества:

- бинокуляр позволяет проводить более качественный осмотр объекта;
- меньшая утомляемость оператора по сравнению с монокулярами (нет необходимости закрывать один глаз);
- зелёная подсветка позволяет находить видеокамеры, защищённые специальными полосовыми фильтрами, используемыми для противодействия всем обнаружителям, использующим только красную подсветку;
- встроенный аккумулятор позволяет не заботиться об элементах питания;
- 6,5 кратное увеличение позволяет детально рассмотреть самые мелкие и труднодоступные элементы интерьера.

Обнаружитель «Оптик-2» безопасен для кратковременной прямой засветки глаз. Лазерное излучение не используется.

1.7. СПЕКТР-PROFESSIONAL Многоканальный комплекс поиска устройств негласного съема информации.

Многоканальный комплекс поиска устройств негласного съема информации «Спектр-Professional» предназначен для выявления излучений радиомикрофонов различных типов, радиостетоскопов, скрытых беспроводных видеокамер, а также обнаружения «опасных» сигналов от устройств негласного съема информации в сети 220В, в слаботочных линиях (пожарная и охранная сигнализации, телефонные линии) и инфракрасном диапазоне.

Комплекс радиомониторинга использует несколько пространственно разнесенных антенн для поиска, оценки параметров и идентификации источников радиоизлучений на частотах 10-3000 МГц. С помощью дополнительного встроенного радиоприемного модуля границы частотного диапазона расширяются до 21000 МГ ц.

Встроенный автоматический конвертор проводных линий (КПЛ) комплекса «Спектр-Professional» обеспечивает обнаружение «опасных» сигналов от сетевых микрофонов в различных проводных линиях, а подключение ИК-датчика позволяет выявлять устройства негласного съема информации в инфракрасном диапазоне.

Скорость панорамного обзора в одноканальной конфигурации составляет до 1100 МГц/с при разрешении по частоте 2 кГц. Высокая производительность дает возможность

комплексу обнаруживать сигналы от радиомикрофонов работающих в режиме накопления информации и кратковременной передачи её в эфир.

Обнаружение и различение сигналов выполняется цифровым параллельным анализатором спектра с разрешением 2 кГц. Высокое разрешение цифрового анализатора спектра позволяет различать и обнаруживать узкополосные сигналы от радиомикрофонов, работающих рядом с легальными радиосредствами.

Специализированное программное обеспечение комплекса позволяет обнаруживать и идентифицировать сигналы от различных типов устройств негласного съема информации, в том числе использующих цифровые виды модуляции, шумоподобную структуру, режим псевдослучайной перестройки рабочей частоты, сверхкоротких посылок (СКП) и т.д. Для обнаружения «опасных» сигналов в программном обеспечении реализован уникальный алгоритм разнесенного приема, имеющий три разновидности.

С помощью встроенной системы видеозахвата многоканальный комплекс поиска устройств негласного съёма информации «СПЕКТР-PROFESSINAL» выводит на экран управляющего компьютера продетектированное изображение от скрытых беспроводных видеокамер. Обнаруженный сигнал может быть записанным на жесткий диск компьютера для последующего анализа.

Компактные габаритные размеры, небольшая масса и удобство коммутации аппаратуры позволяют использовать многоканальный комплекс радиомониторинга «Спектр-Professional» в качестве мобильного поискового прибора.

Аппаратура комплекса может питаться от сети 220В, бортовой сети автомобиля (+12В) или встроенной аккумуляторной батареи.

8. Профессиональный детектор скрытых видеокамер DV - 002 (1мГц - 6.5гГц)

Профессиональный современный, компактный, легкий в использовании универсальный детектор беспроводных скрытых видеокамер:

модель DV - 002 прибор предназначен для обнаружения, беспроводных подслушивающих устройств и проводных, беспроводных скрытых видеокамер. Профессиональный детектор скрытых видеокамер/жучков работает от аккумуляторной батареи, которой хватает на 5 часов непрерывной работы. Защита от прослушки сегодня - единственный способ обезопасить себя от вмешательства посторонних в свою личную жизнь.

Основным достоинством данного детектора является его портативность и миниатюрность при том, что он обнаруживает жучки и беспрводные видеокамеры по радиоизлучению, проводные скрытые видеокамеры по бликам линз. Прибор прост и надежен в эксплуатации, небольшого размера 6.5 х 5 х 1.5 см вы можете всегда носить его с собой, это очень важно, потому что скрытые камеры могут находится практически везде.

Технические характеристики:

Работа детектор жучков и скрытых видеокамер основана на принципе оптического сканирования и сканирования радио эфира. Он сканирует эфир на частотах от 10гц до 6500 мгц. Это самый большой диапазон сканирования из всех приборов.

Прибор имеет 2 степени индикации: световая и звуковая. Поиск осуществляется по принципу обнаружения световых блик, отраженные от линз, которыми оснащены все объективы, и по принципу тепло-теплее-горячо, электромагнитное излучение от передатчиков. На расстоянии от 10-1000 см. в зависимости от мощности передатчика дальность мощностью 5 мВт не менее 5 м, прибор начинает издавать звуковой или световой сигнал.

2. Практическая часть:

2.1. Выполните задание и законспектируйте этапы выполнения.

2.2. Контрольные вопросы.

1. Основные способы обнаружения скрытых видеокамер.
2. Обнаружение скрытого видеонаблюдения с помощью индикатора поля.
3. Обнаружение скрытого видеонаблюдения оптическим способом.
4. Обнаружение скрытого видеонаблюдения электромагнитным обнаружителем видеокамер.
5. Дальность обнаружения скрытых видеокамер.
6. Время и условия обнаружения скрытых видеокамер.
7. Особенности обнаружения при разных принципах действия.
8. Оптико-электронные приборы для дистанционного обнаружения систем скрытого видеонаблюдения.
9. Оптико-электронные прибор «АНТИСВИД». Принцип действия и основные характеристики.
10. Профессиональные обнаружители скрытых видеокамер.
11. «ОПТИК - 2». Принцип действия и основные характеристики.
12. Многоканальные комплексы поиска устройств негласного съема информации.
13. Спектр - PROFESSIONAL. Принцип действия и основные характеристики.
14. Профессиональные детекторы скрытых видеокамер.
15. «ODV-2». Принцип действия и основные характеристики.
16. Эффект фотовозвращения и его использование в процедурах поиска.
17. Что такое ПЗС-матрица и где она используется?.
18. Выявление видеокамер посредством принципа электромагнитного обнаружения.
19. Методы локализации мест расположения скрытых видеокамер.
20. Технология поиска с использованием оптических обнаружителей.
21. Технология поиска с использованием электромагнитных обнаружителей.

Порядок отчетности и форма контроля выполнения работы

Выполнение лабораторной работы осуществляется в два этапа: на первом этапе изучается теоретический материал по теме лабораторной работы. На втором этапе дается письменный ответ на 4 вопроса из пункта 2.1. Каждый вариант предполагает ответы согласно номеру варианта и далее номера кратные 5. Так, например для первого варианта это вопросы 1, 6, 11, 16, для второго - 2, 7, 12, 17 и т.д.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе».

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1	1-2	1-3	1-3

Оценочные средства: ***отчет.***

Лабораторная работа №3-4
Ознакомление с многофункциональным имитатором сигналов «Шиповник 2»

Цель работы: Ознакомиться с функциональными возможностями многофункционального имитатора сигналов «Шиповник 2»

Порядок выполнения работы

1. Теоретическая часть

1.1. Вместо введения

Информационная безопасность - многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Обеспечение информационной безопасности связано с комплексным решением трех задач, связанных с обеспечением, целостности и конфиденциальности информации. Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Поскольку ущерб субъектам информационных отношений может быть нанесен, опосредовано, через определенную информацию и ее носители (в том числе автоматизированные системы обработки), то закономерно возникает заинтересованность субъектов в обеспечении безопасности этой информации и систем ее обработки и передачи.

Иными словами, в качестве объектов, подлежащих защите в интересах обеспечения безопасности субъектов информационных отношений, должны рассматриваться: информация, ее носители и процессы ее обработки.

Однако всегда следует помнить, что уязвимыми, в конечном счете, являются именно заинтересованные в обеспечении определенных свойств информации и систем ее обработки субъекты.

Поэтому, говоря об обеспечении безопасности информации циркулирующей в системе, необходимо иметь в виду процессы обеспечения безопасности самих субъектов, участвующих в процессах информационного взаимодействия.

В свете сказанного, термин «безопасность информации» нужно понимать как ***защищенность*** информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Поэтому под безопасностью компьютерной системы обработки информации будем понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных и персонала) от подобного рода нежелательных для соответствующих субъектов информационных отношений воздействий.

Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Доступность - это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени.

Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило.

Целостность информации условно подразделяется на статическую и динамическую.

Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность - гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность информации. Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе. *Конфиденциальность* это гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности.

Кроме этого, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

Наибольшую сложность при решении вопросов обеспечения безопасности конкретных информационно-управляющих систем (информационных технологий) представляет задача определения реальных требований к уровням защиты критичной для субъектов информации, циркулирующей в АС. Ориентация на интересы субъектов информационных отношений дает ключ к решению данной задачи для общего случая.

1.2. Ознакомление с многофункциональным имитатором сигналов «Шиповник - 2»

К многофункциональным имитаторам сигналов, средств нелегального съема информации, работающих по радиоканалу, выпускаемых отечественной промышленностью, относятся, в первую очередь, Шиповник-1 и Шиповник-2.

Изделие "Шиповник-1" предназначено для проверки эффективности работы устройств и комплексов радиомониторинга, используемых для обследования и защиты выделенных помещений, а также для обучения специалистов, занимающихся поиском каналов утечки информации.

Имитатор радиосигналов "Шиповник-1" представляет собой маломощный радиопередатчик с узкополосной ЧМ.

В приборе реализована возможность выбора вида модулирующего сигнала, который поступает либо от встроенного свип-генератора звуковой частоты либо с микрофонного канала. Наличие свиппирующего сигнала позволяет легко идентифицировать имитатор, а микрофонный канал представляет собой удобное средства проверки акустической завязки у комплексов радиомониторинга.

Шиповник-2 Имитатор работы средств нелегального съема информации, работающих по радиоканалу. Предназначен для проверки эффективности работы устройств и комплексов радимониторинга, используемых для обследования и защиты выделенных помещений, а также для обучения специалистов, занимающихся поиском каналов утечки информации.

"Шиповник-2" отличается широким набором функций и представляет собой маломощный передатчик, работающий в нескольких диапазонах частот, в котором реализованы различные виды модуляции и имеется возможность задания типа модулирующего сигнала.

Прибор имеет встроенный микропроцессор, жидкокристаллический дисплей, отображающий режимы работы имитатора, и клавиатуру, с помощью которой оператор может задавать параметров работы устройства.

ТЕСТ 031

Контрольное устройство ТЕСТ 031 предназначено для контроля многофункциональных поисковых устройств (ST 031, ST 031P и ST 032). Его использование позволяет оценить работоспособность следующих режимов:

- высокочастотного детектора-частотомера;
- анализатора проводных линий (АПЛ);
- детектора низкочастотных магнитных полей;
- детектора инфракрасных излучений.

ТЕСТ 031 так же может применяться для проверки других устройств с аналогичными каналами обнаружения.

ТЕСТ 031 представляет собой комплект имитаторов, собранных в одном корпусе с автономным питанием.

Имитатор для оценки работоспособности высокочастотного детектора-частотомера представляет собой минирадиопередатчик с кварцевой стабилизацией частоты и возможностью отключения модулирующего сигнала, для анализатора проводных линий - генератор сигнала с заданной частотой, для детектора низкочастотных магнитных полей - источник стабильного магнитного поля и для детектора инфракрасных излучений - передатчик ИК-диапазона с заданной частотой поднесущей.

ТЕСТ 031 позволяет оценить чувствительность тестируемого тракта, точность сопутствующих измерений (частотомера, синтезатора АПЛ), работоспособность детекторов, осциллографа, спектроанализатора и отображения результатов измерений.

Для формирования и излучения в эфир радиосигналов, имитирующих работу любых типов радиопередающих устройств, в том числе:

- с накоплением информации и последующей её передачей в эфир (сигналы со сверхкороткой передачей - СКП);
- с псевдослучайной скачкообразной перестройкой несущей частоты радиосигнала (ППРЧ);
- с непосредственным расширением спектра исходного сигнала модуляцией несущей частоты псевдослучайной М-последовательностью (шумоподобных сигналов - ШПС);
- с амплитудной модуляцией радиосигнала; с частотной модуляцией радиосигнала;
- с фазовой модуляцией радиосигнала;
- с частотной манипуляцией радиосигнала (FSK передатчик);
- с фазовой манипуляцией радиосигнала (PSK передатчик);
- с амплитудно-фазовой манипуляцией радиосигнала (QAM передатчик);
- работающих в режиме многоканальных систем с частотным разделением каналов (ЧРК-ЧМ передатчик);
- работающих в режиме многочастотной передачи (МЧ передатчик);
- работающих в режиме многоканальных систем с кодовым разделением каналов (CDMA передатчик);
- со структурой, эквивалентной шумовому сигналу (ГШ передатчик);
- стандарта GSM/DCS;
- стандарта Bluetooth;
- сигналов черно-белых видеокамер.

Параметры сигналов задаются и загружаются с помощью внешней ПЭВМ. Особенности комплекса:

- возможность формирования радиосигналов с любыми заданными оператором спектральными характеристиками;
- наличие библиотеки стандартных сигналов, возможность создания пользовательских библиотек сигналов;
- возможность работы в автоматизированном режиме по заданным оператором программам излучения сигналов;
- размещение в защищенном кейсе, возможность работы в полевых условиях;
- возможность скрытого применения для проверки реакции созданной системы защиты информации.

Может использоваться для проверки эффективности распределенных систем радиомониторинга крупных объектов; подготовки операторов поиска сложных видов сигналов современных закладочных устройств.

1.3. Органы управления имитатором.

На верхней панели имитатора расположены (рис.1):

1 - ЖКИ дисплей;
2 - клавиатура;
3 - светодиодный индикатор;
4 - тумблер включения устройства.

На левой боковой панели располагаются:

5 - антенна диапазона 144 МГц;
6 - антенна диапазона 433 МГц;
7 - антенна диапазона 1200/2400 МГц;

На правой боковой панели установлены:

8 - разъем для подключения сетевого адаптера 15 В/1,2 А;

9 - разъем RS232 для связи с персональным компьютером;

10 - разъем для подключения внешнего НЧ сигнала

11 - микрофон

Рис. 1. Внешний вид имитатора

1.4. Подготовка имитатора к работе и работа с ним.

Подсоедините антенны к имитатору в соответствии с рис.1.

Перед началом эксплуатации устройства зарядите встроенный аккумулятор. Для этого подключите сетевой адаптер к разъему (8) и включите адаптер в розетку сети электропитания. Переключатель питания (4) должен находиться в положении “0”.

Для полной зарядки разряженного аккумулятора необходимо около 8 часов. Во время зарядки на дисплее (1) отображается сообщение “Зарядка Аккум. в процессе”, и мигает светодиодный индикатор (3).

Цвет индикатора показывает состояние аккумулятора на данный момент: Красный - аккумулятор разряжен полностью, желтый - разряжен частично, зеленый - заряжен.

После окончания зарядки на дисплее (1) появится сообщение “Зарядка Аккум. окончена”, а светодиодный индикатор (3) переходит в режим постоянного свечения зеленым цветом.

Примечание. Допускается эксплуатация имитатора от сетевого адаптера с одновременной подзарядкой аккумулятора.

Включение устройства осуществляется переводом переключателя питания (4) в положение “1”, при этом на дисплей (1) сначала выводится приветствие, а затем он переходит в режим отображения служебной информации.

Светодиодный индикатор (3) показывает состояние аккумулятора на данный момент (см. п.7.2.).

Дисплей (1) отображает следующую информацию в шести информационных полях, разделенных пробелами (поля располагаются слева - направо в две строки соответственно):

верхняя строка: поле А - Диапазон частот излучаемого сигнала. поле Б - Вид модуляции (тип) сигнала. поле В - Состояние таймера.

нижняя строка: поле Г - Источник модулирующего сигнала. поле Д - Активность/пассивность инвертора спектра. поле Е - Состояние (режим) передатчика.

Клавиатура (2) предназначена для управления прибором и имеет 15 кнопок.

№ кнопки	**Название**	**Функция кнопки**
1	«144 МГц»	Установка диапазона частот передатчика на 144 МГ ц. Выбранный диапазон отображается в поле А дисплея (1).
2	«433 МГц»	Установка диапазона частот передатчика на 433 МГ ц. Выбранный диапазон отображается в поле А дисплея (1).
3	«1.2ГГц»	Установка диапазона частот передатчика на 1.2 ГГц. Выбранный диапазон отображается в поле А дисплея (1).
4	«2.4ГГц»	Установка диапазона частот передатчика на 2.4 ГГц. Выбранный диапазон отображается в поле А дисплея (1).
5	«узк. Чм/широк. Чм»	Установка вида модуляции. Нажатие на эту кнопку устанавливают ЧМ модуляцию с узкой или широкой полосой соответственно. Выбранный вид модуляции отображается в поле Б дисплея (1)
6	«Дельта мод. /ЧМ-ЧМ»	Нажатие на эту кнопку позволяют выбрать Дельта модуляцию или ЧМ-ЧМ модуляции.
6	«ППРЧ»	Включение ППРЧ
7	«ШПРС»	Включение ШПС «ШПРС»
9	«ж»	Увеличение длительности включения таймера. Выбранная позиция отображается в поле В дисплея (1)
10	«О»	Уменьшение длительности включения таймера. Выбранная позиция отображается в поле В дисплея (1)
11	«Пуск»	Запуск передатчика.
12	«Стоп»	Выключение передатчика.
13	«Источник сигнала»	Выбор источника модулирующего сигнала (см. 7.6.). Выбранный источник отображается в поле Г дисплея (1)
14	«Инверсия спектр»	Включение/выключение инвертора спектра. Состояние инвертора отображается в поле Д дисплея (1)
15	«Подсветка»	Включение/выключение подсветки дисплея.

После включения прибора передатчик находится в режиме ожидания, об этом свидетельствует сообщение “Стоп” в поле Е дисплея (1).

Запуск передатчика прибора производится нажатием кнопки «Стоп» клавиатуры (2). Устройство переходит в режим излучения с выбранными характеристиками. На дисплее в этом режиме в поле Е дисплея (1) отображается сообщение «Излучение».

Перевод обратно в режим ожидания производится нажатием кнопки «Стоп» клавиатуры или автоматически по таймеру.

В режиме излучения кнопки выбора диапазона и вида модуляции заблокированы. Для изменения этих параметров необходимо выйти из режима излучения в режим ожидания. Все остальные параметры допускается изменять во время излучения.

Таймер имеет 12 временных значений. Позиция “Т—с” означает, что таймер отключен, и выход в режим ожидания осуществляется только нажатием кнопки «Стоп».

С помощью кнопок “ж” и «о» можно менять значения таймера, время отображается в секундах в поле В дисплея.

После нажатия кнопки «Пуск» имитатор перейдет в режим излучения и значение числа оставшихся секунд начнет уменьшаться. При достижении таймером нуля, устройство перейдет в режим ожидания.

При нажатии на кнопку «Пуск» во время излучения устройство входит в режим периодического излучения. В этом режиме когда таймер доходит до нуля, передатчик отключается, а таймер взводится и снова начинает отсчет, по достижении нуля вновь включает передатчик и т.д. Такой режим возможен, только если выбранное время больше секунды.

Выбор источника сигнала производится с помощью кнопки «Источник сигнала».

Всего есть пять источников сигнала:

- Встроенный микрофон (11).
- Встроенный свип-генератор.
- Встроенный свип-генератор + динамик.
- Левый линейный вход разъема 10
- Правый линейный вход разъема 10

Инвертор спектра включается/выключается нажатием кнопки «Инверсия спектр». Инверсия распространяется на все перечисленные в пункте выше источники сигнала.

2. Практическая часть:

2.1. Выполните задание и законспектируйте этапы выполнения.

2.2. Контрольные вопросы.

1. Три глобальные задачи информационной безопасности.
2. Объекты и субъекты информационной безопасности.
3. Уровни безопасности субъектов и объектов доступа.
4. Статическая и динамическая целостность безопасности.
5. Конфиденциальность информации в автоматизированных системах.
6. Функциональные характеристики многофункциональных имитаторов «Шиповник 1».
7. Функциональные характеристики многофункциональных имитаторов «Шиповник 2».
8. Основные характеристики контрольного устройства ТЕСТ 0.31.
9. Особенности подготовки имитатора к работе.
10. Функциональное назначение кнопок клавиатуры имитатора.

11. Характеристики режимов излучения имитатора.
12. Характеристики встроенного свин-генератора.
12. Характеристики встроенного инвертора спектра.
12. Выбор диапазона - особенности и характеристики.
13. Режим выбора вида модуляции и его характеристики.
13. Характеристики и функциональные возможности режима Дельта-модуляции.
14. Характеристики и функциональные возможности режима ЧМ модуляции.
14. Установка диапазона частот передатчика.
15. Выбор источника модулирующего сигнала.
15.
16. Проверка эффективности распределенных систем радиомониторинга больших
16.
16. – Методики поиска сложных видов сигналов закладных устройств

Порядок отчетности и форма контроля выполнения работы

Выполнение лабораторной работы осуществляется в два этапа: на первом этапе изучается теоретический материал по теме лабораторной работы. На втором этапе дается письменный ответ на 4 вопроса из пункта 1.3. Каждый вариант предполагает ответы согласно номеру варианта и далее номера кратные 5. Так, например для первого варианта это вопросы 1, 6, 11, 16, для второго - 2, 7, 12, 17 и т.д.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе»

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1	1-2	1-3	1-3

Оценочные средства: ***отчет.***

Лабораторная работа № 4-5 Работа с устройствами комбинированной защиты объектов информатизации.

Цель работы:

Ознакомиться с функциональными возможностями и работой устройств комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН “Соната-РК1” и “Соната-РК2”.

Порядок выполнения работы

1. Теоретическая часть

1.1. *Устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН “Соната-РК1” и “Соната-РК2”.*

Устройства комбинированной защиты "Соната-РК1" и "Соната-РК2" предназначены для защиты информации, обрабатываемой основными техническими средствами и системами до 1 -йкатегории включительно, от утечки за счет ПЭМИН путем постановки маскирующих помех в линиях электропитания и заземления, а также путем пространственного зашумления и частичного поглощения информативных сигналов, распространяющихся по линиям электропитания и заземления.

Устройства "Соната-РК1" и "Соната-РК2" соответствует требованиям "Норм эффективности защиты АСУ и ЭВМ от утечки информации за счет побочных электромагнитных излучений и наводок" и технических условий ЮДИН.665820.002 ТУ и ЮДИН.665820.006 ТУ соответственно. Устройства могут использоваться для защиты объектов ЭВТ, а также устанавливаться в выделенных помещениях до 1 категории

включительно без принятия дополнительных мер защиты акустической речевой информации. Соответствие подтверждается сертификатами ФСТЭК России (№ 954 на "Соната-РК1", № 2168 на "Соната-РК2").

Особенности конструкции устройств "Соната-РК1" и "Соната-РК2" позволяют получать эффективное и недорогое решение задачи комплексной защиты ("ПЭМИ + наводки на ВТСС и их линии + наводки на линии электропитания и заземления") объекта вычислительной техники состоящего из одиночного средства вычислительной техники в ситуациях, когда остро стоит проблема помех, создаваемых генераторами маскирующего шума.

Устройства "Соната-РК1" и "Соната-РК2" являются комбинацией фильтра поглощающего типа, генераторов шумового тока с корректировкой спектра и регулировкой интегрального уровня и элементов антенной системы (см функциональную схему рис 1).

При этом:

1) передаточная характеристика фильтра и частотный спектр мощности маскирующей помехи взаимно дополняют друг друга (рис 2);

2) предусмотрена возможность избирательной корректировки спектральной плотности шума в 3-полосах с целью с целью минимизации ухудшения электромагнитной обстановки объекта;

3) обеспечивается "накачка" электромагнитной энергией шума элементов защищаемого технического средства (ТС) с целью создания помехи в комбинированных (и/или не учтенных) технических каналах "утечки" информации.

Соната-РК1. Вид спереди.

Соната-РК1. Вид сзади.

Соната-РК2. Вид спереди

Соната-РК2. Вид сзади

Для наиболее полного использования возможностей устройства защищаемое ОТС необходимо подключать как указано на фото 1.1 и 1.2.

Фото 1.1.

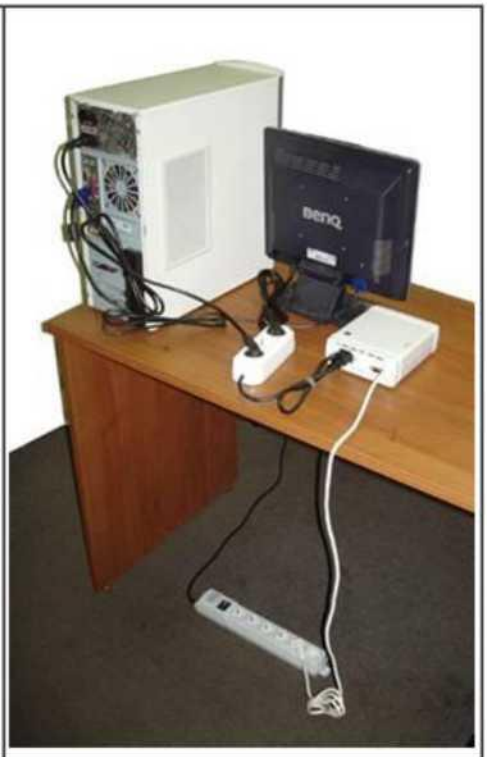


Фото 1.2.

1.2. *Подготовка устройства к работе и работа с ним.*

Устройства могут быть использованы как объектовый генератор шумового ЭМИ. Для этого в сетевой выход необходимо включить более ни к чему не подключенный сетевой шнур от компьютера и вытянуть всю конструкцию в вертикальную прямую линию (рис. 3). Располагать генераторы целесообразно вдоль границы КЗ.

Если розетку сети 220В выбрать на границе КЗ (по аналогии с изделием "Соната-РС1"), то устройство будет работать и в качестве объектового генератора шума по сети электропитания и линиям заземления.

Подготовка и установка устройства осуществляются согласно рисунку 3.

Сертификаты:

Соната-РК1 - Сертификат ФСТЭК № 954 **от 05.11.2004 (до 05.11.2016)**

Соната-РК2 - Сертификат ФСТЭК № 2168 **от 13.09.2010 (до 13.09.2016)**

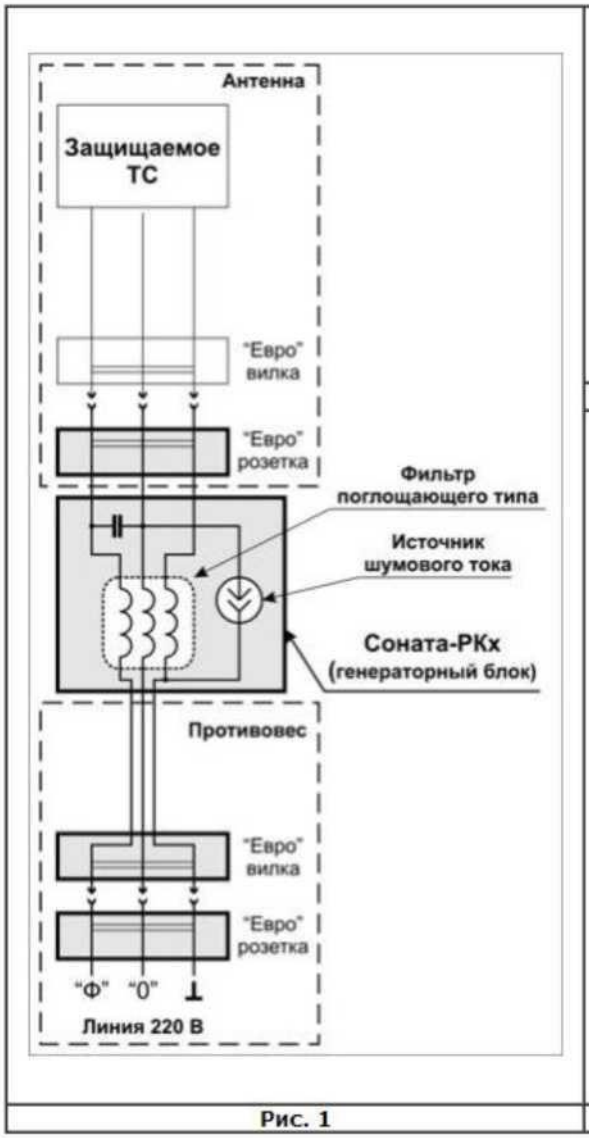


Рис. 1

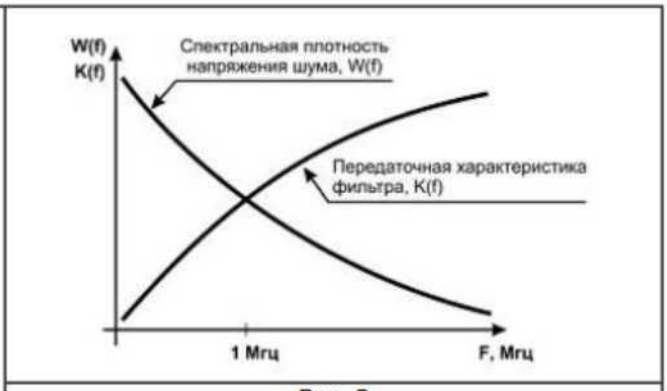


Рис. 2

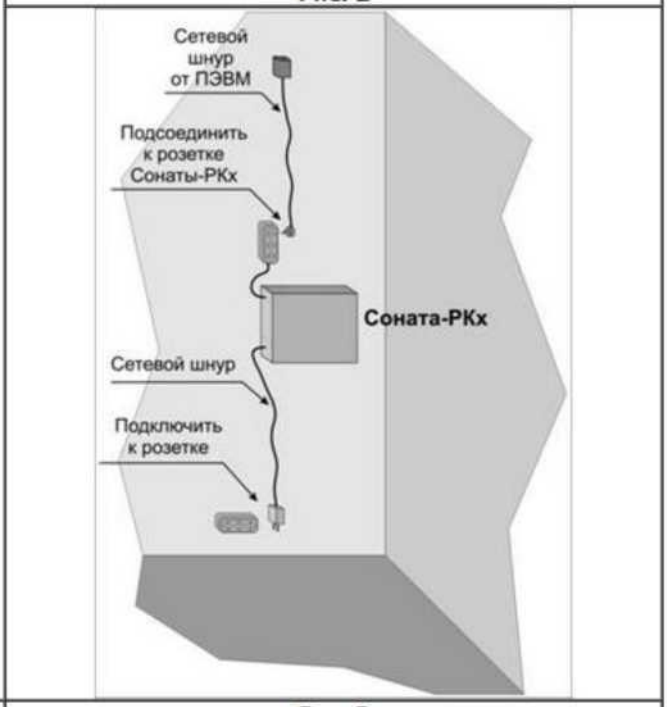


Рис. 3

1.3. *Основные технические характеристики.*

Основные технические характеристики изделия "Соната-РК1" :

Параметр	**Значение**
Диапазон генерируемых частот	0,01.1000 МГц
Спектральная плотность мощности радиоизлучения, дБ относительно 1 мкВ/м^кГц , на расстоянии 1 м не менее	
- в полосе 0,1 ... 0,3 МГ ц	60
- в полосе 0,3 ... 30 МГ ц	50
- в полосе 30 ... 300 МГ ц	45
- в полосе 300 ... 1000 МГц	30
Спектральная плотность напряжения шумов на нагрузке 3 Ом, дБ относительно 1 мкВ^кГц, не менее:	
- в полосе 0,01 ... 0,15 МГц	35
- в полосе 0,15 ... 30 МГц	50
- в полосе 30 МГц ... 1000 МГц	35

Диапазон плавного регулирование уровня шума на выходе устройства, не менее, дБ: - в полосе "А" (ориентировочно 0,01 ... 1,5 МГц) - в полосе "В" (ориентировочно 0,1 ... 30 МГц) - в полосе "С" (ориентировочно 30 ... 1000 МГц)	 15 10 10
Коэффициент направленного действия в горизонтальной плоскости, не более *	4
Коэффициент качества шума, не менее	0,8
Коэффициент межспектральных корреляционных связей шума, не более	2
Максимальная мощность нагрузки, подключаемой через изделие.	1 кВт
Электропитание изделия	сеть ~220В / 50 Гц
Мощность потребляемая от сети, Вт, не более	10
Габаритные размеры	142 х 60 х 167 мм
Продолжительность непрерывной работы, не менее	24 ч

Основные технические характеристики изделия "Соната-РК2":

Параметр	**Значение**
Диапазон генерируемых частот, МГ ц	0,01.2000
Спектральная плотность напряженности электрической составляющей электромагнитного поля, дБ (мкВ/м/ '^кГц), не менее: - в полосе 0,01 - 3,5 - в полосе 3,5 - 100 - в полосе 100 - 1000 - в полосе 1000 - 1700 - в полосе 1700 - 2000	 60 50 40 35 30
Спектральная плотность напряженности магнитной составляющей электромагнитного поля, дБ (мкВ/м/ '^кГц), не менее: - в полосе0,01 - 0,25 - в полосе 0,25 - 1 - в полосе 1.0 - 15 - в полосе 15 - 30	 50 40 35 30
Спектральная плотность напряжения шумов в линиях электропитания, дБ (мкВ^кГц), не менее: - в полосе 0,01 - 0,02 - в полосе 0,02 - 1 - в полосе 1 - 100 - в полосе 100 - 1000 - в полосе 1000 - 1500 - в полосе 1500 - 2000	 50 60 50 40 30 20
Коэффициент направленного действия в горизонтальной плоскости, не более	9 2
Коэффициент качества шума, не менее	0,9
Коэффициент межспектральных корреляционных связей шума, не более	2
Сигнализация неисправностей (снижение уровня шума более чем на 50 %, переход к генерации в многомодовом режиме)	Встроенная свето-звуковая
ДУ интерфейс *)	НР - контакт
Мощность нагрузки, подключаемой через изделие, кВт, не более	1

Электропитание изделия	сеть ~220 В / 50 Гц
Мощность потребляемая от сети, Вт, не более	10
Габаритные размеры	142 х 60 х 167 мм
Продолжительность непрерывной работы, час, не менее	8

3.4. Комплекс ТСЗИ 2051 «Соната-РК2» + ДУ по ИК-каналу

Задача: Обеспечить возможность удаленной беспроводной активации/деактивации одиночного ТСЗИ, предназначенного для защиты объектов информатизации до 1 категории включительно от утечки информации за счет наводок на линии электропитания и заземления и утечки информации за счет побочных электромагнитных излучений и наводок.

Специальные требования к непрерывному автоматизированному контролю исполнения команд ДУ и исправности устройства *не предъявляются.*

Решение: Для решения поставленной задачи мы предлагаем схему, основанную на устройстве комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН «Соната-РК2» исп. 205, которое может управляться с помощью изделия «Соната-ДУ21М» исп. 510 по ИК-каналу.

Информацию об изменении режима работы и исправности управляемого изделия Пользователь получает путем визуального наблюдения за сигнализацией на передней панели управляемого изделия и (или) по звучанию встроенной звуковой сигнализации.

Схема решения для изделия «Соната-РК2» исп. 205 показана на Рис.1.

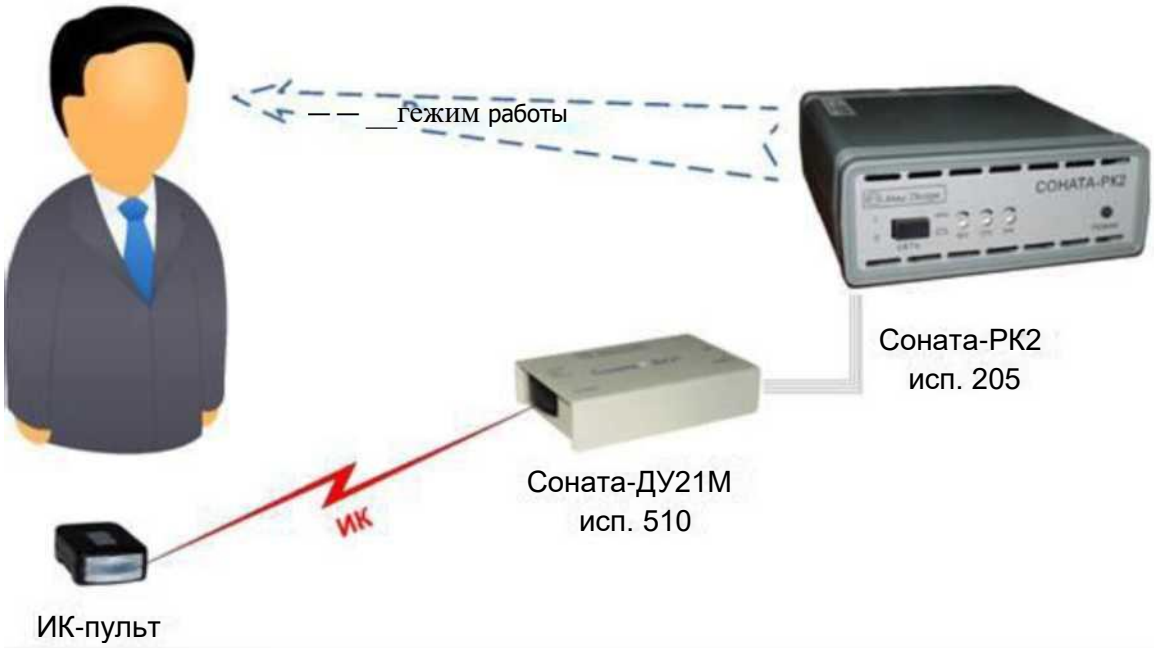


Рис. 3

Перечень устройств:

Обозначение на схеме	Полное наименование (комментарии)	ID	Максимальное количество
Соната-РК2 исп. 205	"Соната-РК2". Устройство комбинированной защиты объектов информатизации от утечки информации.	205	1
Соната-ДУ21М исп. 510	"Соната-ДУ", мод ДУ21М, исп. 510. Аппаратура ДУ (ИК-канал)	510	1
ИК-пульт	Пульт управления ИК 2-кнопочный	513	1*)

2. Практическая часть:

2.1. Выполните задание и законспектируйте этапы выполнения.

2.2. Контрольные вопросы.

1. Устройство комбинированной защиты «Соната - РК1».
2. Функциональные возможности и основные технические характеристики устройства.
3. Подготовка устройства к работе и работа с ним..
4. Область применения устройства.
5. Устройство комбинированной защиты «Соната - РК2».
6. Функциональные возможности и основные технические характеристики устройства.
7. Подготовка устройства к работе и работа с ним..
8. Область применения устройства.
9. Комбинированный генератор защиты «Соната - 2Р».
10. Функциональные возможности и основные технические характеристики генератора.
11. Подготовка генератора к работе и работа с ним.
12. Область применения генератора.
13. Комплекс ТСЗИ 2051 «Соната - РК2» + ДУ по ИК-каналу.
14. Функциональные возможности и основные технические характеристики комплекса.
15. Подготовка комплекса к работе и работа с ним..
16. Область применения комплекса.
17. Устройство комбинированной защиты «Соната - РК1».
18. Функциональные возможности и основные технические характеристики устройства.
19. Подготовка устройства к работе и работа с ним.
20. Область применения устройства.

Порядок отчетности и форма контроля выполнения работы

Выполнение лабораторной работы осуществляется в два этапа: на первом этапе изучается теоретический материал по теме лабораторной работы. На втором этапе дается письменный ответ на 4 вопроса из пункта 1.3. Каждый вариант предполагает ответы согласно номеру варианта и далее номера кратные 5. Так, например для первого варианта это вопросы 1, 6, 11, 16, для второго - 2, 7, 12, 17 и т.д.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе».

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1	1-2	1-3	1-3

Оценочные средства: ***отчет.***

Лабораторная работа №7-8. «Аттестации помещения по требованиям безопасности информации»

Цель работы:

- изучить системы аттестации объектов информации;
- изучить защиты звонковой и микрофонной цепей;
- освоить процесс разработки комплексных схем защиты.

1. Теоретическая часть

1.1. Система аттестации объектов информации.

Деятельность по аттестации объектов информатизации по требованиям безопасности информации осуществляет ФСТЭК России. Дадим определение объекта информатизации.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Аттестация объектов информатизации (далее аттестация) - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России). Наличие аттестата соответствия в организации дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате.

Аттестация производится в порядке, установленном "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 года. Аттестация должна проводиться до начала обработки информации, подлежащей защите. Это необходимо в целях официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте информатизации.

Аттестация является обязательной в следующих случаях:

- государственная тайна;
- при защите государственного информационного ресурса;
- управление экологически опасными объектами;
- ведение секретных переговоров.

Во всех остальных случаях аттестация носит добровольный характер, то есть может осуществляться по желанию заказчика или владельца объекта информатизации.

Аттестация предполагает комплексную проверку (аттестационные испытания) объекта информатизации в реальных условиях эксплуатации. Целью является проверка соответствия применяемых средств и мер защиты требуемому уровню безопасности. К проверяемым требованиям относится:

- защита от НСД, в том числе компьютерных вирусов;
- защита от утечки через ПЭМИН;
- защита от утечки или воздействия информацию за счет специальных устройств, встроенных в объект информатизации.

Аттестация проводится органом по аттестации в соответствии со схемой, выбираемой этим органом, и состоит из следующего перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Органы по аттестации должны проходить аккредитацию ФСТЭК в соответствии с "Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации".

Все расходы по проведению аттестации возлагаются на заказчика, как в случае добровольной, так и обязательной аттестации.

Органы по аттестации несут ответственность за выполнение своих функций, за сохранение в секрете информации, полученной в ходе аттестации, а также за соблюдение авторских прав заказчика.

1.2.Организационная структура системы аттестации объектов информатизации.

В структуру системы аттестации входят:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - ФСТЭК России;
- органы по аттестации объектов информатизации по требованиям безопасности информации;
- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации.

В качестве органов по аттестации могут выступать отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры ФСТЭК России, которые прошли соответствующую аккредитацию.

Органы по аттестации:

- аттестуют объекты информатизации и выдают "Аттестаты соответствия";

• осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

• отменяют и приостанавливают действие выданных этим органом "Аттестатов соответствия";

• формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

• ведут информационную базу аттестованных этим органом объектов информатизации;

• осуществляют взаимодействие с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.

ФСТЭК осуществляет следующие функции в рамках системы аттестации:

• организует обязательную аттестацию объектов информатизации;

• создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;

• устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;

• организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;

• аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;

• осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;

• рассматривает апелляции, возникающие в процессе аттестации объектов информатизации, и контроля за эксплуатацией аттестованных объектов информатизации;

• организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

Испытательные лаборатории проводят испытания несертифицированной продукции, используемой на аттестуемом объекте информатизации.

Со списком органов по аттестации и испытательных лабораторий, прошедших аккредитацию, можно ознакомиться на официальном сайте ФСТЭК России в разделе "Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации".

Заявители:

• проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

• привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;

• предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

• привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

• осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия";

• извещают орган по аттестации, выдавший "Аттестат соответствия", обо всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации;

• предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

Для проведения испытаний заявитель предоставляет органу по аттестации следующие документы и данные:

• приемо-сдаточную документацию на объект информатизации;
• акты категорирования выделенных помещений и объектов информатизации;
• инструкции по эксплуатации средств защиты информации;
• технический паспорт на аттестуемый объект;
• документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;
• сертификаты соответствия требованиям безопасности информации на ВТСС;
• сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;
• акты на проведенные скрытые работы;
• протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);
• протоколы измерения величины сопротивления заземления;
• протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
• данные по уровню подготовки кадров, обеспечивающих защиту информации;
• данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;
• нормативную и методическую документацию по защите информации и контролю эффективности защиты.

Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией:

• пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
• перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
• перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
• перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
• перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
• перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
• схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
• технологические поэтажные планы здания с указанием мест расположения объектов информатизации и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;

• планы объектов информатизации с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;

• план-схему инженерных коммуникаций всего здания, включая систему вентиляции;

• план-схему системы заземления объекта с указанием места расположения заземлителя;

• план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;

• план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;

• план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;

• схемы систем активной защиты (если они предусмотрены).

1.3. Порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

• подача и рассмотрение заявки на аттестацию. Заявка имеет установленную форму, с которой можно ознакомиться в "Положении об аттестации объектов информатизации по требованиям безопасности". Заявитель направляет заявку в орган по аттестации, который в месячный срок рассматривает заявку, выбирает схему аттестации и согласовывает ее с заявителем.

• предварительное ознакомление с аттестуемым объектом - производится в случае недостаточности предоставленных заявителем данных до начала аттестационных испытаний;

• испытание в испытательных лабораториях несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.

• разработка программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.

• заключение договоров на аттестацию. Результатом предыдущих четырех этапов становится заключение договора между заявителем и органом по аттестации, заключением договоров между органом по аттестации и привлекаемыми экспертами и оформлением предписания о допуске аттестационной комиссии к проведению аттестации.

• проведение аттестационных испытаний объекта информатизации. В ходе аттестационных испытаний выполняется следующее:

  o анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

  o определяется правильность категорирования объектов ЭВТ и классификации АС (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

о проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

о проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

о проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

о оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протокол аттестационных испытаний должен включать:

- вид испытаний;
- объект испытаний;
- дату и время проведения испытаний;
- место проведения испытаний;
- перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
- перечень нормативно-методических документов, в соответствии с которыми проводились испытания;
- методику проведения испытания (краткое описание);
- результаты измерений;
- результаты расчетов;
- выводы по результатам испытаний.

Протоколы испытаний подписываются экспертами - членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов.

Заключение по результатам аттестации подписывается членами аттестационной комиссии, утверждается руководителем органа аттестации и представляется заявителю. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Порядок выполнения работы

1. Составить самостоятельно документацию на контролируемое помещение, изучить ее, определить возможные разведоопасные направления и возможные виды разведки.
2. Изобразить план-схему исследуемого помещения.
3. На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения (Гастроль-П) и металодетектора.
4. Сделать выводы по результатам проделанной работы и подготовить отчет.

Подготовка отчета.

При подготовке отчета по лабораторной работе необходимо:

1. Придерживаться рекомендаций, указанных в Лабораторном практикуме.

2. Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.
3. Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.
4. Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Контрольные вопросы

1. Система аттестации объектов информации.
2. Организационная структура системы аттестации объектов информатизации.
3. Порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1	1-2	1-3	1-3

Оценочные средства: ***отчет.***

Лабораторная работа № 9-10. «Технические средства защиты информации в телефонных линиях»

Цель работы:

Приобрести практические работы с техническими средствами защиты информации в телефонных линиях.

1. Теоретическая часть

1.1. Защита телефонных аппаратов.

При защите телефонных линий как каналов утечки информации необходимо учитывать следующее:

1) телефонные аппараты (даже при положенной трубке) могут быть использованы для перехвата акустической речевой информации из помещений, в которых они установлены, то есть для подслушивания разговоров в этих помещениях;

2) телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания акустических закладок, установленных в этих помещениях, а также для передачи перехваченной информации;

3) возможен перехват (подслушивание) телефонных разговоров путем гальванического или через индукционный датчик подключения к телефонной линии закладок (телефонных ретрансляторов), диктофонов и других средств несанкционированного съема информации.

Телефонный аппарат имеет несколько элементов, способных преобразовывать акустические колебания в электрические сигналы (микрофонный эффект). К ним относятся звонковая цепь, телефонный и, конечно, микрофонный капсюли. За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы. При положенной трубке телефонный и микрофонный капсюли гальванически отключены от телефонной линии и при подключении к ней специальных высокочувствительных низкочастотных усилителей возможен перехват опасных сигналов, возникающих в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ.

При использовании для съема информации метода "высокочастотного навязывания", несмотря на гальваническое отключение микрофона от телефонной линии, сигнал навязывания благодаря высокой частоте проходит в микрофонную цепь и модулируется по амплитуде информационным сигналом. Следовательно, в телефонном аппарате необходимо защищать как звонковую цепь, так и цепь микрофона.

Для недопущения несанкционированного использования ТЛ применяются следующие технические способы (ТС):

• применение пассивных ТС защиты: сигнализаторов подключения, обрыва лини, счетчиков времени разговора, в т.ч. по межгороду;

• применение активных ТС защиты: устройства защиты от параллельного подключения, блокираторы выхода на межгород, устройства кодирования доступа к телефонной линии, устройства активного маскирования информации и др.

Пассивные ТС защиты телефонной линии.

К наиболее широко применяемым пассивным методам защиты относятся:

- ограничение опасных сигналов;
- фильтрация опасных сигналов;
- отключение преобразователей (источников) опасных сигналов;

Ограничения опасных сигналов основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме ограничителя малых амплитуд используются два встречновключенных диода. Диоды имеют большое сопротивление для токов малой амплитуды и единицы - для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную линию и практически не оказывает влияние на прохождение через диоды полезных сигналов.

Диодные ограничители включаются последовательно в линию звонка. Фильтрация опасных сигналов используется главным образом для защиты телефонных аппаратов от "высокочастотного навязывания".

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов. Емкость конденсаторов выбирается такой величины, чтобы зашунтировать зондирующие сигналы высокочастотного навязывания и не оказывать существенного влияния на полезные сигналы. Обычно для установки в звонковую цепь используются конденсаторы емкостью 1 мкФ, а для установки в микрофонную цепь - емкостью 0,01 мкФ. Более сложное фильтрующее устройство представляет собой многозвенный фильтр низкой частоты на LC-элементах.

Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель.

Отключение телефонных аппаратов от линии при ведении в помещении конфиденциальных разговоров является наиболее эффективным методом защиты информации.

Реализация этого метода защиты заключается в установке в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке.

В дежурном режиме (при положенной телефонной трубке) телефонный аппарат отключен от линии, и устройство находится в режиме анализа поднятия телефонной трубки и наличия сигналов вызова. При этом сопротивление развязки между телефонным аппаратом и линией АТС составляет не менее 20 МОм. Напряжение на выходе устройства в дежурном приеме составляет 5...7В. При получении сигналов вызова устройство переходит в режим передачи сигналов вызова, при котором через электронный коммутатор телефонный аппарат подключается к линии.

Подключение осуществляется только на время действия сигналов вызова. При поднятии телефонной трубки устройство переходит в рабочий режим и телефонный аппарат подключается к линии. Переход устройства из дежурного в рабочий режим осуществляется при токе в телефонной линии не менее 5 мА. Изделие устанавливается в разрыв телефонной линии, как правило, при выходе ее из выделенного (защищаемого) помещения или в распределительном щитке (кроссе), находящемся в пределах контролируемой зоны.

Контроль состояния телефонной линии и обнаружение атак осуществляется посредством применения аппаратуры контроля линий связи:

- индикаторных устройств;
- анализаторов проводных линий и кабельных локаторов (рефлекторметров и устройств, использующих принципы нелинейной локации);
- универсальных комплексов контроля.

Для проведения углубленных исследований телефонных линий на предмет обнаружения несанкционированных подключений подслушивающих устройств используется более серьезная аппаратура, эффективная работа с которой доступна только специалистам. Это анализаторы телефонных линий и кабельные локаторы.

При использовании стандартных анализаторов телефонных линий можно эффективно обнаруживать наличие радиозакладных устройств с непосредственным подключением телефонной линии. Единственное неудобство - необходимость предварительного обесточивания проверяемой линии.

Телефонный анализатор в простейшем виде представляет собой комбинацию мультиметра и прибора, позволяющего обнаруживать переделки в телефонном аппарате. С помощью мультиметра отмечаются отклонения от нормальных значений ряда параметров (например, напряжения) абонентской линии связи при снятой и положенной телефонной трубке. Повышенное или пониженное по сравнению со стандартным значением напряжение или сопротивление может означать, соответственно, параллельное или последовательное подключение подслушивающих устройств. Существуют анализаторы, способные инициировать работу РЗУ и тем самым выявлять подслушивающие устройства, приводимые в действие от сигнала вызова уже с помощью детекторов поля или устройств радиоконтроля.

Рефлектометр (или «кабельный радар») позволяет определять расстояние до подозрительного места в телефонной линии. Принцип его действия основан на том, что в линию посылается импульс, который отражается от неоднородностей сети, возникающих в местах параллельного и последовательного подключения к ней различных дополнительных устройств. Расстояние до места подключения определяется по положению отраженного импульса на экране электронно-лучевой трубки, зависящему от времени задержки отраженного импульса.

При применении универсальных комплексов контроль осуществляется по изменению уровня сигнала на входе приемника контроля в момент поднятия трубки. Если в линии установлено РЗУ, то процесс поднятия трубки сопровождается существенным изменением уровня принимаемого излучения, кроме того в наушниках прослушивается тональный сигнал номеронабирателя либо другой тестовый сигнал. В «чистой» линии имеет место только кратковременный скачок излучения в момент поднятия трубки (в наушниках слышен короткий щелчок), а тональный набор не прослушивается. Для обеспечения благоприятных условий проверки целесообразно антенну приемника контроля держать как можно ближе к элементам телефонной сети проводу, аппарату, трубке, распределительной коробке и т. д., последовательно перемещая ее от одной точки контроля к другой.

1.2. Защита звонковой цепи. Защита микрофонной цепи.

Защита звонковой цепи. Причиной появления канала утечки информации являются электроакустические преобразования. При разговоре в помещении акустические колебания воздействуют на маятник звонка, соединенного с якорем электромагнитного реле. Под воздействием звуковых сигналов якорь совершает микроколебания, что, в свою очередь, вызывает колебания якорных пластин в электромагнитном поле катушек, следствием чего становится появление микротоков, промодулированных звуком. Амплитуда ЭДС, наводимой в линии, для некоторых типов телефонных аппаратов может достигать нескольких милливольт. Для приема используется низкочастотный усилитель с частотным диапазоном 300-3500 Гц, который подключается к абонентской линии.

Для защиты от такого канала утечки информации используется схема, представленная на рис. 1.1.

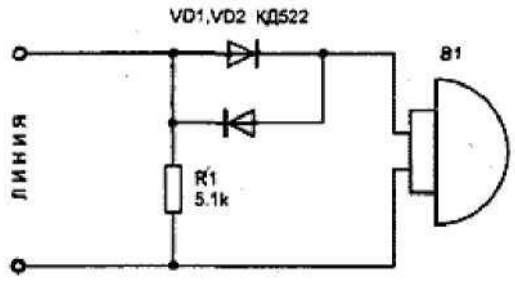


Рис 1.1. Схема защиты звонковой цепи

Два кремниевых диода VD1 и VD2 включены встречно-параллельно в цепь звонка телефонного аппарата B1. Они образуют зону нечувствительности для микро-ЭДС. Это объясняется тем, что в интервале 0-0,65 В диод обладает большим внутренним сопротивлением (вольтамперная характеристика диодов представлена на рис. 5.2

Поэтому низкочастотные токи, наводимые в схеме аппарата, не пройдут в линию. В то же время звуковой сигнал абонента и напряжение вызова свободно "проходят" через диоды, так как их амплитуда превышает порог открывания диодов VD1, VD2. Резистор R1 является дополнительным шумящим элементом. Подобная схема, включенная последовательно в линию связи, подавляет микроЭДС катушки на 40-50 дБ.

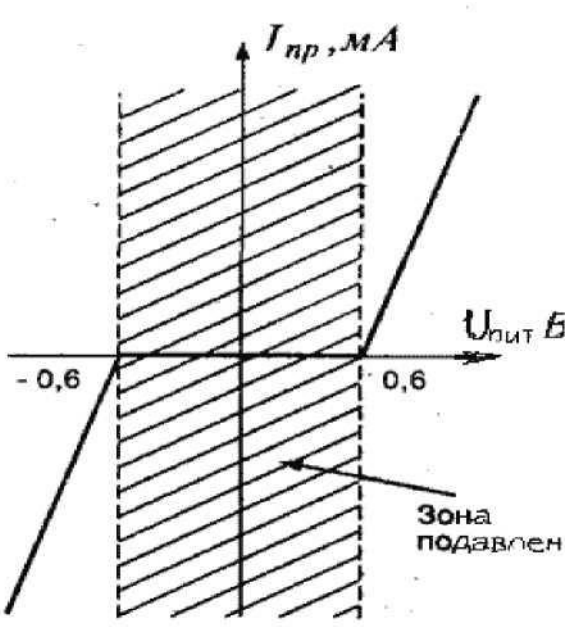


Рис. 1 .2. Вольтамперная характеристика диодов

Вместо указанных на схеме диодов можно использовать диоды Д226, КД105, КД102.

Защита микрофонной цепи. Этот вариант получения информации связан с явлением, так называемого высокочастотного навязывания. При этом относительно общего корпуса на один провод подается высокочастотное колебание (частотой более 150 кГц). Через элементы схемы телефонного аппарата, даже если трубка не снята, высокочастотные колебания поступают на микрофон, где и модулируются звуковыми колебаниями. Прием информации производится относительно общего корпуса через второй провод линии. Амплитудный детектор позволяет выделить низкочастотную огибающую Для дальнейшего усиления и записи. Схема защиты телефонного аппарата от этого метода съема информации представлена на рис. 1.3..

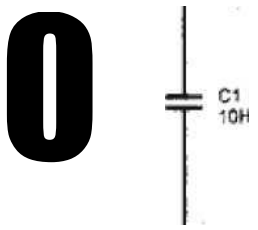


Рис. 1.3. Схема защиты микрофона

Так как модулирующим элементом является микрофон М1 телефонного аппарата, то для его защиты достаточно подключить параллельно микрофону М1 конденсатор С1 емкостью 0,01-0,05 мкФ. При этом конденсатор С1 шунтирует по высокой частоте микрофонный капсюль М1. Глубина модуляции высокочастотных колебаний уменьшается более чем в 10000 раз, что делает практически невозможной дальнейшую демодуляцию.

0.3. Комплексная схема защиты. Защита линий связи. Световой анализатор телефонной линии.

Эта схема представляет собой сочетание приведенных ранее двух схем. Кроме конденсаторов и резисторов схема, представленная на рис. 1.4, содержит катушки индуктивности.

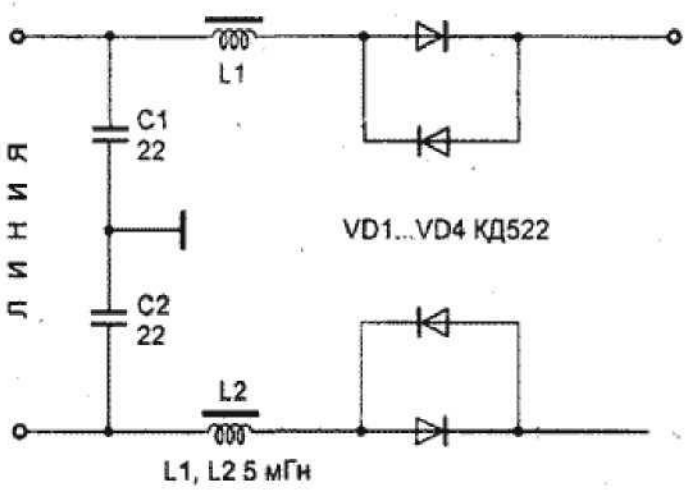


Рис. 1 .4. Комплексная схема защиты

Диоды VD1-VD4, включенные встречно-параллельно, защищают звонковую цепь телефона. Конденсаторы и катушки образуют фильтры C1, L1 и C2, L2 для подавления напряжений высокой частоты.

Детали монтируются в отдельном корпусе навесным монтажом. Устройство не нуждается в настройке. Однако оно не защищает пользователя от непосредственного подслушивания - путем прямого подключения в линию.

Кроме рассмотренной схемы существует и ряд других, которые по своим характеристикам близки к ранее описанным устройствам. Ниже приведены схемы (рис. 1.5), предназначенные для комплексной защиты телефонных аппаратов и линий связи и часто используемые в практической деятельности.

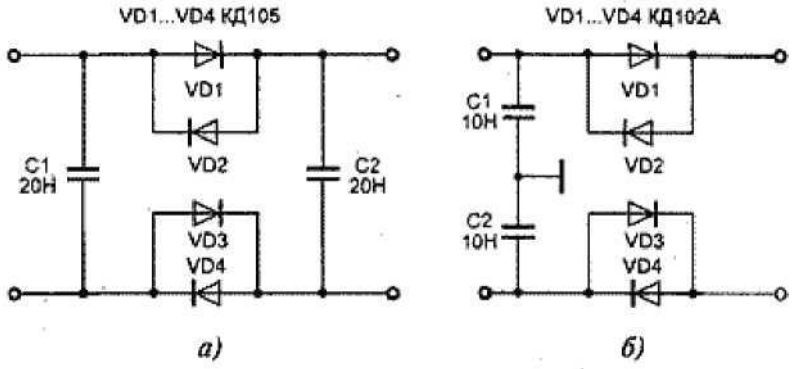


Рис. 1.5. Схема комплексной защиты

0.4. Индикатор линии на микросхеме. Активный индикатор состояния линии.

Активный индикатор состояния линии в отличие от выше приведенного устройства не только выявляет подключение дополнительной нагрузки, но и при срабатывании системы сигнализации переводит устройство в активный режим работы. Этот режим позволяет блокировать многие радиоретрансляционные устройства и приборы, предназначенные для автоматической записи телефонных переговоров. Принципиальная схема такого устройства представлена на рис. 1.6.

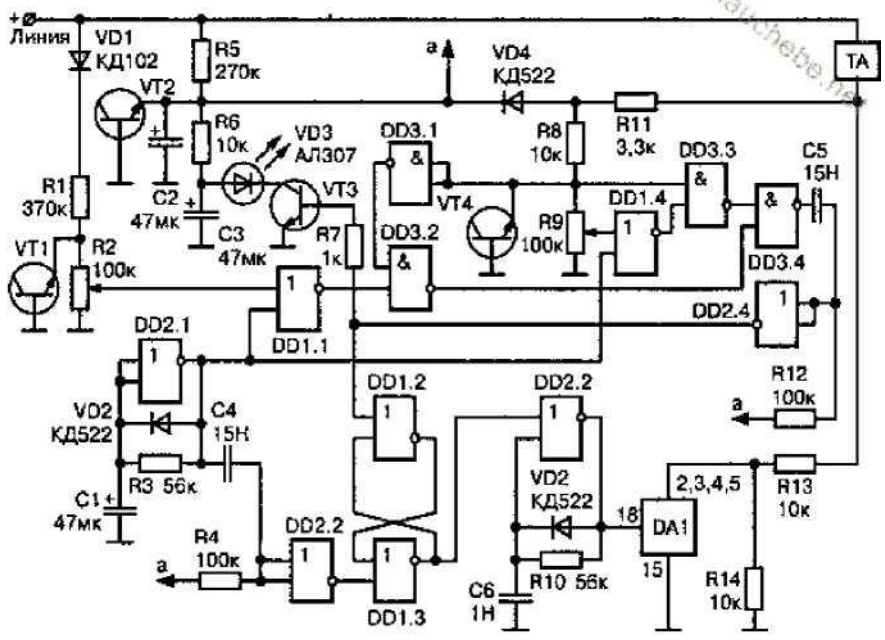


Рис. 1.6 Активный индикатор состояния линии

Устройство собрано на 4 микросхемах и 4 транзисторах. Исходное состояние: трубка телефонного аппарата опущена. Питание устройства осуществляется от телефонной линии через ограничительный резистор R5. Конденсатор С2 заряжается через резистор R5 до напряжения стабилизации стабилитрона, выполненного на транзисторе VT2.

С конденсатора С2 напряжение величиной 7—8 В поступает на устройство для питания микросхем (точка а). От источника питания через резистор R6 заряжается конденсатор С3. Резисторы R6, R7, конденсатор С3, светодиод VD3 и транзистор VT3 образуют схему индикации устройства.

Напряжение линии через диод VD1 типа КД102 поступает на делитель напряжения, образованный резисторами R1 и R2. Напряжение на резисторе R2 ограничивается транзистором VT1, включенным по схеме стабилитрона до напряжения питания, что необходимо для защиты входов микросхем от высокого напряжения.

С движка подстроечного резистора R2 напряжение высокого уровня поступает на вход элемента DD1.1 микросхемы К561ЛЕ5, запрещая проход импульсов с генератора, выполненного на элементе DD2.1 микросхемы К561ТЛ1. Этот генератор собран на основе триггера Шмидта. При заряде и разряде конденсатора С1 на выходе генератора появляются прямоугольные импульсы.

Поскольку заряд конденсатора С1 происходит через диод VD2 типа КД522, а разряд — через резистор R3, то на выходе элемента DD2.1 имеют место короткие положительные импульсы с частотой следования 1—0,5 Гц. Первый же импульс, пройдя через дифференцирующую цепочку С4, R4 и элемент DD2.2, устанавливает триггер, собранный на элементах DD2.1, DD1.3, в положение, когда на входе элемента DD2.3 низкий уровень напряжения. Генератор, собранный на DD2.3, выключен и на выводах 1, 8 микросхемы DA1 типа КР1014КТ1 присутствует высокий уровень. Одновременно импульсы с DD2.1 поступают на элементы DD1.1 и DD1.4. Через DD1.1 импульсы не проходят, так как с резистора R2 поступает высокий уровень.

Нулевой уровень, снимаемый с резистора R9, подается на входы элементов DD3.1 и вход DD3.3 микросхемы К561ЛА7. Поэтому импульсы, проходящие через DD1.4, не проходят на DD3.4. Следовательно, на выходе DD2.4 присутствует логический нуль, и транзистор VT3 закрыт. С движка резистора R2 снимается напряжение логической единицы, достаточное для переключения элемента DD1.1, выполняющего функцию управляемого компаратора с чувствительностью в десятки милливольт.

Примечание. Если к линии подключается дополнительная нагрузка сопротивлением менее 100 кОм, то напряжение в линии уменьшится на некоторую величину.

Одновременно уменьшается и напряжение на движке резистора R2. Это приводит к появлению на входе DD1.1 напряжения, воспринимаемого микросхемой как уровень логического нуля. Этот уровень- разрешает прохождение импульсов от DD2.1 через DD1.1. Поскольку на выходе DD3.1 высокой уровень, то импульсы проходят через ключ DD3.2. При этом на выходе DD3.3 тоже высокий уровень и эти импульсы проходят и через ключ DD3.4.

Продифференцированные импульсы цепочкой С6, R12 и элементом DD2.4 поступают на базу транзистора VT3. Транзистор открывается, и конденсатор С3 быстро разряжается через открытый транзистор VT3 и светодиод VD3, который ярко вспыхивает с частотой 0,5—1 Гц. В перерывах между импульсами конденсатор С3 подзаряжается через резистор R6. Так как оценка состояния линии происходит под управлением импульсов с генератора DD2.1, то некоторое изменение напряжения в линии в момент заряда конденсатора С3 на работе устройства не сказывается.

Рассмотрим случай, когда телефонная трубка снята. При этом сопротивление телефонного аппарата включается между плюсовым проводом линии и резисторами R11 и R13. Напряжение в линии уменьшается до 5—25 В, так как нагрузкой линии будут телефонный аппарат, резистор R13 и резистор R14, зашунтированный малым (около 10 Ом) сопротивлением микросхемы DA1.

Напряжение, снимаемое с резистора R13, обеспечивает питание устройства через диод VD4 типа КД522. При этом . напряжение высокого уровня с точки соединения резисторов R8, R9 поступает на элементы DD3.3 и DD3.1. Низким уровнем закрывается ключ DD3.2. С движка резистора R9 снимается напряжение логической единицы, близкое к напряжению переключения компаратора DD1.4. Допустим, что к линии подключается (или была подключена) дополнительная параллельная или последовательная нагрузка, которая приводит к уменьшению напряжения в линии.

При этом напряжение на движке резистора R9 принимает уровень, расцениваемый микросхемой как уровень логического нуля. При этом импульсы с DD2.1 проходят через DD1.4, DD3.3 и DD3.4. После дифференцирующей цепочки С6, R12 и элемента DD2.4 они поступают на базу транзистора VT3, включая световую индикацию. Одновременно первый же импульс переводит триггер на DD1.2 и DD1.3 в состояние, разрешающее работу генератора на элементе DD2.3. С выхода генератора короткие импульсы частотой 12—20 кГц поступают на ключ, выполненный на микросхеме DA1.

Ключ начинает закрываться и открываться с частотой генератора. При этом сигнал в линии модулируется данной частотой, это вызывает расширение спектра сигнала, излучаемого радиоретранслятором, подключенным в линию.

Одновременно напряжение в линии увеличивается до 35—45 В. Это связано с тем, что последовательно с резистором R13 включается резистор R14, ранее шунтированный ключом DA1. Повышение напряжения в линии до такого уровня позволяет нейтрализовать автоматические записывающие устройства, срабатывающие по уровню напряжения в линии.

Для того чтобы работа этого генератора не мешала анализу состояния линии, он периодически отключается путем переключения триггера DD1.2, DD1.3 на момент оценки состояния линии. Если в процессе оценки состояния линии принимается решение о том, что линия свободна от посторонних подключений, то схема автоматически устанавливается в исходное состояние и переходит в ждущий режим с периодической проверкой состояния линии.

Детали. Резисторы используются типа МЛТ-0,125. Диод VD1 можно заменить на КД105, Д226. Транзисторы можно заменить на КТ3102, КТ503. Микросхемы можно использовать из Серий 564 и 1561. Конденсаторы Cl, С2 и СЗ должны быть с минимальным током утечки.

Настройка. При настройке устройства устанавливается частота генераторов 0,5—1 Гц и 12—20 кГц резисторами R3 и R10, соответственно. При включенном генераторе DD2.3 резистором R14 устанавливается уровень напряжения в линии, равный 35—45 В, при котором еще не происходит рассоединения линии. Исходные уровни срабатывания рассматриваемого устройства устанавливаются резисторами R2 и R9.

2. Порядок выполнения лабораторной работы.

2.1. Работа с устройством защиты телефонных линий от прослушивания «ПРОКРУСТ».

1. *Подготовка к работе.*

2.1.1.Собрать лабораторную установку в соответствии с рис.2. 1.

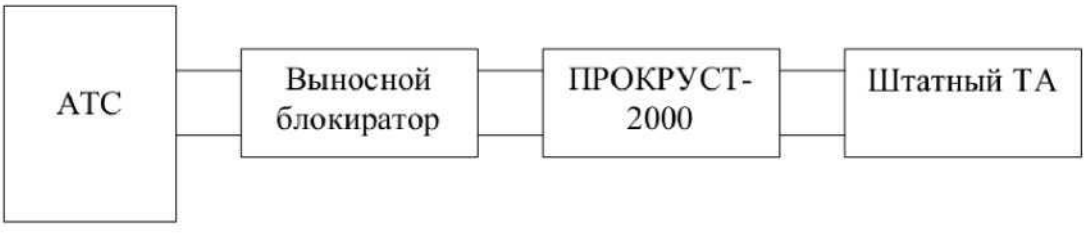


Рис. 2.1.

2.1.2. Перевести выключатель в положение ВКЛЮЧЕНО, при этом кнопка ЗАЩИТА засветится красным цветом, кнопки ДЕТЕКТОР, ПОМЕХА, УРОВЕНЬ засветятся и погаснут, а цифровой дисплей вольтметра отобразит значение напряжения на телефонной линии порядка 50-60 В. Снять телефонную трубку и убедиться в наличии гудка, при этом цифровой дисплей вольтметра покажет напряжение порядка 10-15 В, световой индикатор БЛОКИРОВКА засветится непрерывным красным цветом, кнопка УРОВЕНЬ замигает и через 4-5 секунд погаснет. Положить трубку, после чего вольтметр покажет напряжение порядка 50-60 В, а индикатор БЛОКИРОВКА погаснет.

2.1.3. Проверить работу выносного блокиратора, для чего зафиксировать переключатель БЛОКИРОВКА в нажатом состоянии для блокировки линии (при этом световой индикатор БЛОКИРОВКА засветится непрерывным зеленым цветом, а дисплей вольтметра покажет напряжение от 0 до 1,3 В). После отжатия переключателя БЛОКИРОВКА соответствующий индикатор погаснет, а дисплей вольтметра покажет напряжение порядка 50-60 В.

Снова зафиксировать переключатель БЛОКИРОВКА в нажатом состоянии, снять телефонную трубку, линия разблокируется, и при этом в трубке раздастся непрерывный гудок, индикатор БЛОКИРОВКА засветится непрерывным красным цветом, вольтметр покажет напряжение порядка 10-15 В, кнопка УРОВЕНЬ замигает и через 4-5 секунд погаснет. Положить трубку, линия заблокируется, индикатор БЛОКИРОВКА засветится непрерывным зеленым цветом, вольтметр покажет напряжение порядка 0-1,3 В.

Набрать с другого телефона ваш номер и убедиться в том, что блокиратор разблокирует линию, признаком чего является наличие вызывного звонка на вашем аппарате, при этом индикатор БЛОКИРОВКА засветится непрерывным красным цветом, а кнопка ДЕТЕКТОР замигает и будет мигать до тех пор, пока звонки не прекратятся, или не будет снята телефонная трубка.

После одного из этих событий кнопка будет мигать еще 4-5 секунд и погаснет. Если звонки закончились, а трубку не сняли, линия заблокируется через 4-5 секунд, то же самое произойдет, если после разговора трубка будет положена.

2.1.4. Проверить действия кнопок, для чего ручку УРОВЕНЬ ПОМЕХИ поставить в положение МАКС., снять телефонную трубку, набрать номер абонента, поднять трубку его ТА и после прекращения мигания кнопки УРОВЕНЬ сделать следующее:

- нажать кнопку ДЕТЕКТОР до ее засветки и отпустить, при этом в трубке появится слабый гул, после чего нажать эту кнопку еще раз, пока она не погаснет;
- нажать кнопку ПОМЕХА до ее засветки и отпустить, при этом в трубке появится легкий шум, уменьшить уровень шума ручкой УРОВЕНЬ ПОМЕХИ, и если он уменьшился, то это нормально. Далее установить ручку УРОВЕНЬ ПОМЕХИ в положение МАКС., нажать кнопку ПОМЕХА, пока она не погаснет;
- нажать кнопку УРОВЕНЬ , пока она не засветится, и отпустить, при этом до нажатия этой кнопки вольтметр должен показывать напряжение порядка 10-15 В, а после ее нажатия и отжатия показания вольтметра должны составлять порядка 30-40 В. Далее зафиксировать кнопку СТРОБ в нажатом состоянии, после чего показания вольтметра должны меняться в пределах от 20 до 30 В, прослушать в трубке слабые хлопки с периодичностью около 0,5 секунды. Нажать кнопку УРОВЕНЬ, пока она не погаснет;
- нажать и удерживать кнопку ЗАЩИТА до тех пор, пока не засветятся кнопки ДЕТЕКТОР, ПОМЕХА, УРОВЕНЬ, что свидетельствует о включении полной защиты. Повторное нажатие на эту кнопку приводит к отключению всех режимов защиты.

2.2. Защита телефонных переговоров от прослушивания с использованием радиоизлучающего закладного устройства последовательного подключения (ЗУ1).

2. 2.1. Подготовить прибор «ПРОКРУСТ-2000» к работе, для чего сделать следующее:

- зафиксировать кнопки БЛОКИРОВКА, СТРОБ, Д/У в отжатом состоянии;
- если кнопки ДЕТЕКТОР, ПОМЕХА, УРОВЕНЬ светятся, нажать их до погасания и отпустить;
- зафиксировать показания вольтметра.

2.2.2. Подготовить прибор ST031P к работе, для чего сделать следующее:

- подключить высокочастотную антенну к разъему RF ANT;
- поставить переключатель POWER в положение ON;
- установить порог детектора с помощью кнопок, используя шкалу min - - I - - max, в такое положение, чтобы не было слышно щелчков в акустической системе.

2.2.3.Собрать лабораторную установку в соответствии с рис.2.2.

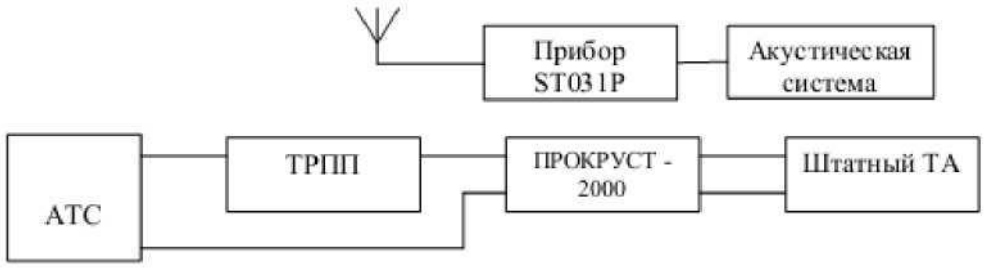


Рис. 2.2

2.2.4. Зафиксировать показание вольтметра и сравнить его с показанием вольтметра в п. 2.1. Сделать вывод о влиянии подключения ТРПП к телефонной линии.

2.2.5. Поднять телефонную трубку, зафиксировать показание вольтметра и сравнить его с показанием вольтметра в п.1.2. Сделать вывод о влиянии подключения ТРПП к телефонной линии.

2.2.6. Манипулируя антенной прибора ST031P, добиться чередующихся тональных посылок (щелчков) в акустической системе, убедиться в том, что по мере приближения антенны к телефонной линии частота щелчков увеличивается, а так же увеличивается число окрашенных сегментов на шкале D индикатора прибора.

2.2.7. На приборе ST031P нажать кнопку ENTER и тем самым выбрать режим AUD, после чего прослушать в акустической системе гудки телефонной линии.

2.3.Защита телефонных переговоров от прослушивания с использованием параллельного ТА.

2. 3.1.Собрать лабораторную установку в соответствии с рис.2.3.

Рис. 2.3.

2. 3.2. Выполнить действия, указанные в п.2.2.1.

2.3.3. Поднять трубку штатного ТА и убедиться в наличии гудка в трубке, при этом индикатор БЛОКИРОВКА будет светиться красным цветом, зафиксировать показание вольтметра. Поднять трубку параллельного ТА, при этом индикатор будет мигать красным цветом, зафиксировать показание вольтметра и сравнить с предыдущим показанием. Положить трубки обоих ТА, индикатор погаснет. Сделать вывод о влиянии подключения параллельного ТА при поднятой трубке штатного ТА.

2.4.Защита телефонной линии от прослушивания с использованием закладного устройства типа «ТЕЛЕФОННОЕ УХО» (ТУ) речевой информации из помещения.

2.4.1.Собрать лабораторную установку в соответствии с рис.2.4.

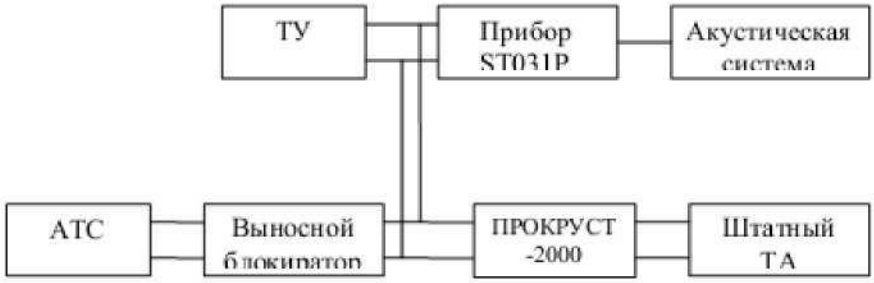


Рис. 2.4.

2.4.2. Выполнить действия, указанные в п.4.3.2.1. Зафиксировать уменьшение показания вольтметра при подключении ТУ к телефонной линии.

2.4.3. Подготовить прибор ST031P к работе, для чего сделать следующее:

- подключить дифференциальный адаптер проводных линий (ДАПЛ) к разъему PROBES;
- подключить ДАПЛ к телефонной линии, используя специальные насадки и розетку, соединенную с телефонной линией.

2. 4.4. Прослушать в акустической системе и просмотреть на экране прибора ST031P речевой сигнал.

2. 4.5. На приборе «ПРОКРУСТ-2000» зафиксировать кнопку БЛОКИРОВКА в нажатом состоянии и убедиться в отсутствии речевого сигнала в акустической системе и на экране прибора ST031P, то есть в прекращении работы закладного устройства ТУ.

2.4.6. На приборе «ПРОКРУСТ-2000» отжать кнопку БЛОКИРОВКА и прослушать речевой сигнал, нажать кнопку ПОМЕХА и убедиться в невозможности слышать речевой сигнал при наличии в акустической системе шумового сигнала.

Содержание отчета

1. Структурные схемы лабораторных установок.
2. Результаты измерений, наблюдений и прослушиваний.
3. Анализ полученных результатов и выводы.

3. Исходные теоретические положения

1. Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных.
2. Дискреционная модель обеспечения целостности данных Кларка-Вильсона.
3. Объекты, требующие контроля целостности (constrained data items), процедуры проверки целостности (integrity verification procedures), корректно сформированные

транзакции (не нарушающие ограничения целостности), тройки "субъект-транзакция-объект".

4. Мандатная модель К.Биба. Уровни целостности данных.
5. Уровни доверия пользователям.
6. Правила мандатного доступа, не нарушающие целостность данных (запрет "чтения вниз", запрет "записи вверх") как инверсия правилам мандатного доступа, не нарушающим конфиденциальность данных (в модели Белла-Лападулы).
7. Проблемы и разновидности совместимости в практической реализации моделей Белла-ЛаПадулы и К.Биба: на основе двух разных решеток безопасности (отдельных систем уровней конфиденциальности и целостности), на основе одной общей решетки, но с двумя отдельными метками для объектов и субъектов (на чтение, на запись).
8. Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах.
9. Принципы "атомарности" (неделимости), "изоляции" транзакций.
10. Нарушения целостности, возникающие при совместной обработке данных, одновременном (параллельном) выполнении транзакций пользователей.
11. Понятие и виды "грязных" (dirty) данных - "грязное чтение" (dirty read), "потерянные изменения" (lost update) и "неповторяющееся чтение" (unrepeatable read).
12. Протоколы выполнения и фиксации транзакций.
13. Протоколы, основанные на "захватах" блокировках объектов.
14. Двухфазной протокол выполнения и фиксации транзакций ("пессимистичный" режим выполнения транзакций).
15. Тупики (Deadlock), их обнаружение и разрушение.
16. Механизмы изоляции транзакций, основанные на временных метках объектов ("оптимистичный" режим выполнения транзакций).

Порядок отчетности и форма контроля выполнения работы

Выполнение лабораторной работы осуществляется в два этапа: на первом этапе изучается теоретический материал по теме лабораторной работы. На втором этапе дается письменный ответ на 4 вопроса из пункта 1.3. Каждый вариант предполагает ответы согласно номеру варианта и далее номера кратные 5. Так, например для первого варианта это вопросы 1, 6, 11, 16, для второго - 2, 7, 12, 17 и т.д.

Контроль выполнения задания производится по окончании занятия и на консультациях в форме защиты выполненной работы, предоставленной в электронном и в бумажном виде в форме «Отчет по лабораторной работе».

Контрольные вопросы

1. Защита телефонных аппаратов.
2. Защита звонковой цепи. Защита микрофонной цепи.
3. Комплексная схема защиты. Защита линий связи. Световой анализатор телефонной линии.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1	1-2	1-3	1-3

Оценочные средства: ***отчет.***

Лабораторная работа № 11-12. «Поиск и измерение побочных электромагнитных излучений и наводок»

Цель работы:

Приобрести практические поиска и измерения побочных электромагнитных излучений и наводок.

1. Теоретическая часть

1.1. Инструментальный контроль утечки информации по техническим каналам: побочные электромагнитные излучения и наводки (ПЭМИН).

К техническим средствам передачи, обработки, хранения и отображения информации ограниченного доступа **(ТСПИ)** относятся:

- технические средства автоматизированных систем управления, электронно-вычислительные машины и их отдельные элементы, в дальнейшем именуемые средствами вычислительной техники (СВТ);
- средства изготовления и размножения документов;
- аппаратура звукоусиления, звукозаписи, звуковоспроизведения и синхронного перевода; системы внутреннего телевидения;
- системы видеозаписи и видео воспроизведения;
- системы оперативно-командной связи;
- системы внутренней автоматической телефонной связи

Данные технические средства и системы в ряде случаев именуются основными техническими средствами и системами**(ОТСС**.

Совокупность средств и систем обработки информации, а также помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, составляет *объект ТСПИ***,** который в некоторых документах называется *объектом информатизации*.

Наряду с техническими средствами и системами, обрабатывающими информацию ограниченного доступа, на объектах ТСПИ также устанавливаются *вспомогательные технические средства и системы* (ВТСС), непосредственно не участвующие в ее обработке.

К ним относятся:

- системы и средства городской автоматической телефонной связи;
- системы и средства передачи данных в системе радиосвязи;
- системы и средства охранной и пожарной сигнализации;
- системы и средства оповещения и сигнализации; контрольно-измерительная аппаратура; системы и средства кондиционирования;
- системы и средства проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, средства радиовещания; телевизоры и радиоприемники и т.д.);
- средства электронной оргтехники;
- системы и средства электрочасофикации и иные технические средства и системы.

В некоторых документах ВТСС называются средствами обеспечения объекта информатизации.

Электропитание ТСПИ и ВТСС, как правило, осуществляется от распределительных устройств и силовых щитов, которые специальными кабелями соединяются с трансформаторной подстанцией городской электросети.

Все технические средства и системы, питающиеся от электросети, должны быть заземлены. Типовая система заземления включает общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с техническими средствами.

Через помещения, в которых установлены технические средства обработки информации ограниченного доступа, как правило, проходят провода и кабели, не относящиеся к ТСПИ и ВТСС, а также металлические трубы систем отопления,

водоснабжения и другие токопроводящие металлоконструкции, которые называются *посторонними проводниками.*

Ряд соединительных линий ВТСС, а также посторонних проводников могут выходить за пределы не только объекта ТСПИ, но и *контролируемой зоны (КЗ),* под которой понимается пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств. Границей контролируемой зоны могут являться периметр охраняемой территории организации, а также ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

Таким образом, при рассмотрении объекта ТСПИ, как объекта разведки, его необходимо рассматривать как систему, включающую:

• технические средства и системы, непосредственно обрабатывающие информацию ограниченного доступа, вместе с их соединительными линиями (под соединительными линиями понимают совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами);

• вспомогательные технические средства и системы вместе с их соединительными линиями;

• посторонние проводники;

• систему электропитания объекта;

• систему заземления объекта.

Для добывания информации, обрабатываемой техническими средствами, “противник” (лицо или группа лиц, заинтересованных в получении этой информации) может использовать широкий арсенал портативных технических средств разведки (ТСР).

Совокупность объекта разведки (в данном случае - объекта ТСПИ), технического средства разведки, с помощью которого добывается информация, и физической среды, в которой распространяется информационный сигнал, называется *техническим каналом утечки информации* (рис. 1.1).

При работе технических средств возникают информативные электромагнитные излучения, а в соединительных линиях ВТСС и посторонних проводниках могут появляться наводки информационных сигналов. Поэтому, технические каналы утечки информации можно разделить на *электромагнитные и электрические.*

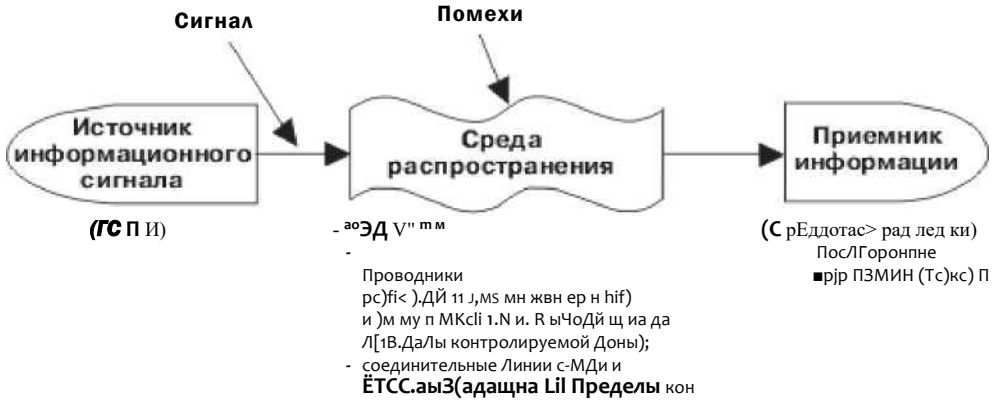


Рис. 1.1. Схема технического канала утечки информации

Электромагнитные каналы утечки информации. В электромагнитных каналах утечки информации носителем информации являются различного вида побочные электромагнитные излучения (ПЭМИ), возникающие при работе технических средств, а именно [4]:

• побочные электромагнитные излучения, возникающие вследствие протекания по элементам ТСПИ и их соединительным линиям переменного электрического тока;

• побочные электромагнитные излучения на частотах работы высокочастотных генераторов, входящих в состав ТСПИ;

• побочные электромагнитные излучения, возникающие как результат паразитной генерации в элементах ТСПИ.

Побочные электромагнитные излучения элементов ТСПИ. В некоторых ТСПИ (например, системах звукоусиления) носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону изменения информационного речевого сигнала. При протекании электрического тока по токоведущим элементам ТСПИ и их соединительным линиям в окружающем их пространстве возникает переменное электрическое и магнитное поле. В силу этого элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ. В состав ТСПИ могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах высокочастотных генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов, которые излучаются в окружающее пространство.

*Побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ***.** Паразитная генерация в элементах ТСПИ, в том числе, самовозбуждение усилителей низкой частоты (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.), возможна за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов.

Частота автогенерации (самовозбуждения) лежит в пределах рабочих частот нелинейных элементов усилителей (например, полупроводниковых приборов, электровакуумных ламп и т.п.). Сигнал на частотах самовозбуждения, как правило, оказывается модулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе усилителя в нелинейный режим работы, т.е. в режим перегрузки.

Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники:

- 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).

Для перехвата побочных электромагнитных излучений ТСПИ “противником” могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН). Как правило, полагается, что ТСР ПЭМИН располагаются за пределами контролируемой зоны объекта.

Качество обнаружения сигнала средством разведки характеризуется вероятностями правильного обнаружения P_o сигнала и ложной тревоги $P_{лт}$**.** Обычно предполагается, что в

средствах разведки используются оптимальные для перехватываемых видов сигналов приемные устройства.

Наиболее часто в них реализуется алгоритм обработки сигнала по критерию Неймана - Пирсона, при котором минимизируется вероятность ошибки 2-го рода (пропуск сигнала) при условии, что вероятность ошибки 1 -го рода (ложная тревога) не больше некоторой заданной величины. Наиболее распространенным видом помех являются внутренние шумы приемного устройства, которые суммируются с принимаемым сигналом (аддитивные шумы). Зная уровень шума приемного устройства, легко рассчитать уровень сигнала на входе приемного устройства, при котором вероятность его правильного обнаружения будет равна некоторому допустимому (нормированному) значению $P_{од_{оп}}$, которое обычно называют чувствительностью приемного устройства $U_{рпм}$.

Для обеспечения требуемого уровня защиты информации допустимое значение вероятности правильного обнаружения сигнала обычно составляет $P_{од_{оп}}=0.1\text{-}0.7$ при $_{-3}$ вероятности ложной тревоги $P_{лт}=10"$.

Используя характеристики приемного устройства и антенной системы средства разведки, можно рассчитать допустимое (нормированное) значение напряженности электромагнитного поля в точке размещения средства разведки, при котором отношение “информационный сигнал/помеха” на входе приемного устройства будет равно некоторому (нормированному) значению, при котором еще возможно или обнаружение средством разведки информационных сигналов с требуемой вероятностью, или измерение их параметров с допустимыми ошибками, а значит - и выделение полезной информации.

Пространство вокруг ТСПИ, в пределах которого напряженность электромагнитного поля превышает допустимое (нормированное) значение, называется **зоной 2 (R2)** [3]. Фактически зона R2 - это зона, в пределах которой возможен перехват средством разведки побочных электрома[illegible]

Рис. 1.2. Перехват побочных электромагнитных излучений ТСПИ средствами разведки ПЭМИН

Зона 2 для каждого ТСПИ определяется инструментально-расчетным методом при проведении специальных исследований технических средств на ПЭМИН и указывается в предписании на их эксплуатацию или сертификате соответствия.

Таким образом, по электромагнитным каналам утечки информации перехват информации может осуществляется путем приема и детектирования средством разведки побочных электромагнитных излучений, возникающих при работе ТСПИ.

Наряду с пассивными способами перехвата информации, обрабатываемой ТСПИ, и рассмотренными выше, возможно использование и активных способов, в частности, способа ***“высокочастотного облучения”*** (рис. 3), при котором ТСПИ облучается мощным высокочастотным гармоническим сигналом (для этих целей используется высокочастотный

генератор с направленной антенной, имеющей узкую диаграмму направленности). При взаимодействии облучающего электромагнитного поля с элементами ТСПИ происходит его переизлучение. На нелинейных элементах ТСПИ происходит модуляция вторичного излучения информационным сигналом. Переизлученный сигнал принимается приемным устройством средства разведки и детектируется.

Рис. 1.3. Перехват информации, обрабатываемой ТСПИ, методом “высокочастотного облучения”

Для перехвата информации, обрабатываемой ТСПИ, также возможно использование электронных устройств перехвата информации (закладных устройств), скрытно внедряемых в технические средства и системы (рис. 4).

Рис. 1.4. Перехват информации, обрабатываемой ТСПИ, путем установки в них закладных устройств

Они представляют собой миниатюрные передатчики, излучение задающих генераторов которых модулируется информационным сигналом. Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается в специальное запоминающее устройство, а уже затем по команде управления передается по радиоканалу.

1.2. Оборудование: анализатор спектра, комплект измерительных антенн, генератор вч сигналов, токосъемник, пробник напряжения, тест-программы.

Существует целый ряд требований от утечки за счет ПЭМИН. Например, информативный сигнал Вашего компьютера не должен выходить за границы контролируемой зоны (КЗ).

Что же для этого предпринимается? А предпринимаются следующие действия...

Прежде всего, для проведения такой работы нам понадобятся следующие устройства:

Рис. 1.5. Анализатор спектра

Рис. 1.6.Комплект измерительных антенн

Рис. 1.7. Генератор ВЧ сигналов

Рис. 1.8. Токосъемник

Рис. 1.9. Пробник напряжения

Теперь, имея всё необходимое можно приступать к работе. Давайте представим что у нас есть автоматизированное рабочее место (АРМ), с расположенным рядом радиатором системы отопления, расстоянием 10м до границ КЗ, и распределительным щитом электропитания на расстоянии 5м от АРМ.

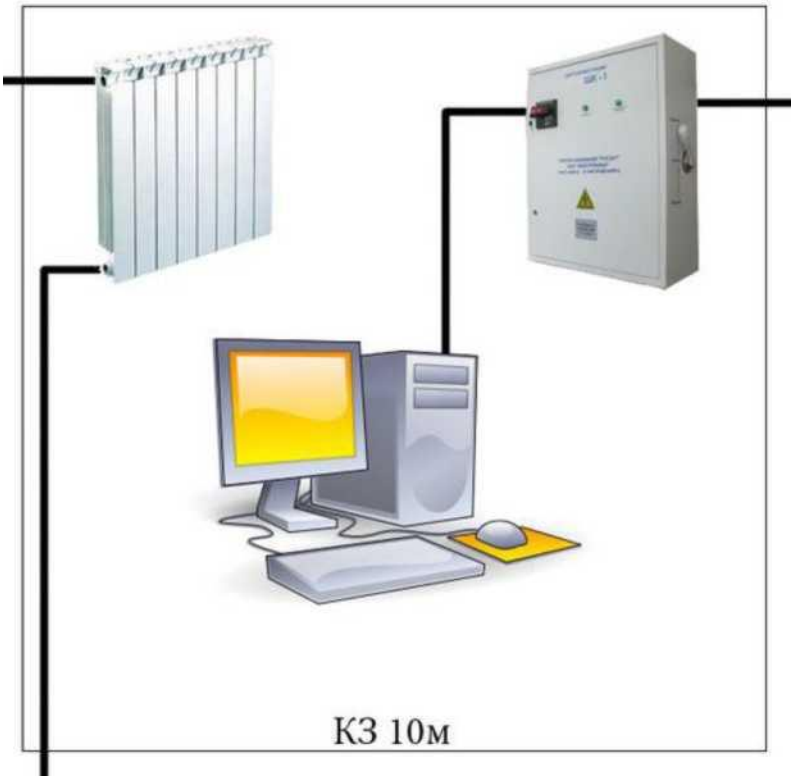


Рис. 1.10. Расположение объекта

И так, запускаем тест-программу. У нас на мониторе возникает вот такая рябь:

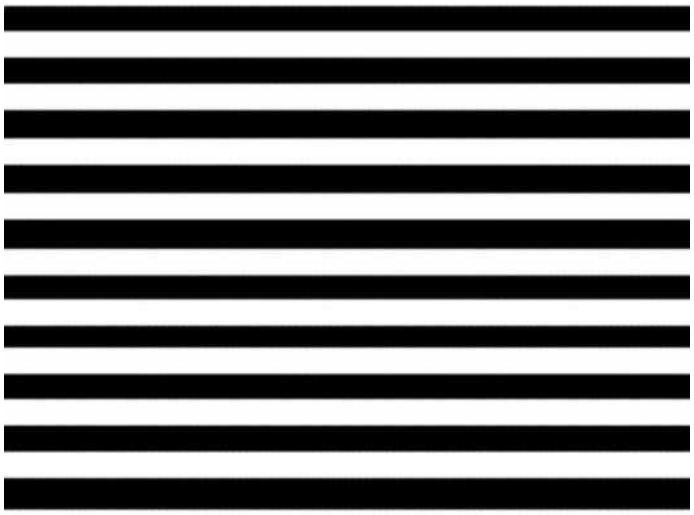


Рис. 1.11. Тест-программа

Тест программа может формировать данную картинку постоянно, а может периодически выключать её, т.е. переставать подавать информативный сигнал. В последнем случае получается мигание картинки на экране монитора.

И так, сформировав постоянный информативный сигнал, начинаем искать его анализатором спектра. При нахождении информативного сигнала монитора, он имеет примерно следующий вид:

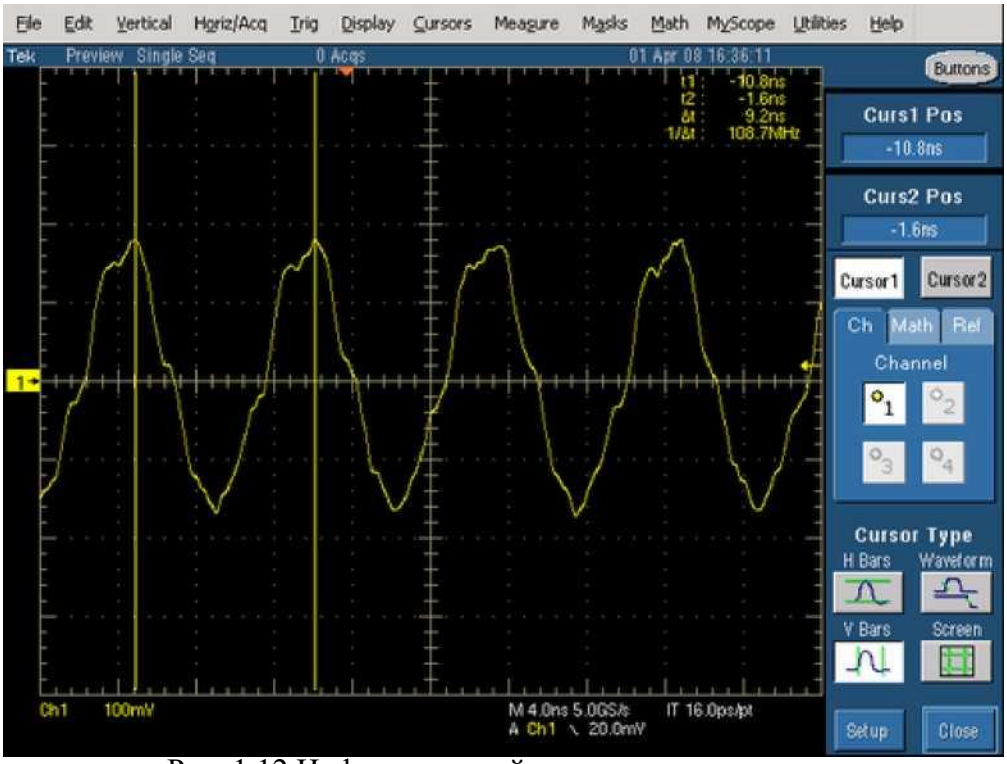


Рис. 1.12.Информативный сигнал монитора

Фиксируем частоту на которой появился сигнал, его уровень и уровень шума. И так пробегаем определенный диапазон частот, в поисках данного сигнала.

Следующим шагом мы делаем замер на радиаторе отопления. Так как АРМ находится близко от радиатора системы отопления, то на нем могут быть наводки информативного сигнала. Частота будет та же, что и на мониторе.

Точно так же ищем сигнал на распределительном щите, каждый раз фиксируя частоту, уровень сигнала и уровень шума. В последствии все эти данные понадобятся для расчетов.

Теперь мы берем генератор ВЧ сигналов, подключаем к нему излучающую антенну и ставим на расстоянии 1м от АРМ. Выставляем максимальную мощность и частоту

информативного сигнала. Берем анализатор с антеннами и измеряем уровень сигнала и шума на границе КЗ.

Далее, мы меняем антенну генератора на токосъемник и фиксируем его на проводе питания АРМ (или на сеттером фильтре). Точно так же подаем сигнал. С анализатором идем на распределительный щит и замеряем уровень сигнала и шума. Можно так же попробовать сделать замер на вводном распределительном устройстве (ВРУ), но туда не всегда есть доступ.

Теперь осталось сделать замер на радиаторе отопления. Токосъемником подаем сигнал генератора на радиатор, а пробником напряжения с анализатором делам замеры. Точно так же делаем замер и на границе КЗ.

Всё! На этом замеры закончены. Теперь нужно произвести расчеты. И выдать протокол инструментального контроля ПЭМИН.

Если у Вас сигнал выходит за границы КЗ Вашей организации, то Вам предпишут установку средств активной защиты, а именно - генератора электромагнитного шума. Данное устройство маскирует информативный сигнал среди огромного количества помех, и найти полезный сигнал уже невозможно.

2. Порядок выполнения лабораторной работы.

2.1. Подготовка комплекса и исследуемого средства к работе

2.1.1. Управляющую ПЭВМ и измерительный прибор необходимо соединить кабелем USB.

2.1.2. Подключить антенну «нулевая диполь» (А117.3) к анализатору спектра R&S FS300 с помощью кабеля А117.3 к разъему (8).

2.1.3. Включить анализатор спектра.

1.4. Включить на исследуемом техническом средстве монитор тест «Зебра».

1.5. Запустить управляющую программу на персональном компьютере.

2.2. Поиск и измерение ПЭМИ в автоматическом режиме измерений

2.2.1. Создание эталона тестового сигнала. Для перехода в полуавтоматический режим измерений выберите в меню главного окна программы пункт «Измерения - Ручной режим» или нажмите соответствующую кнопку быстрого запуска. На экране управляющей ПЭВМ выводится окно полуавтоматического режима, показанное на рис. 2.1.

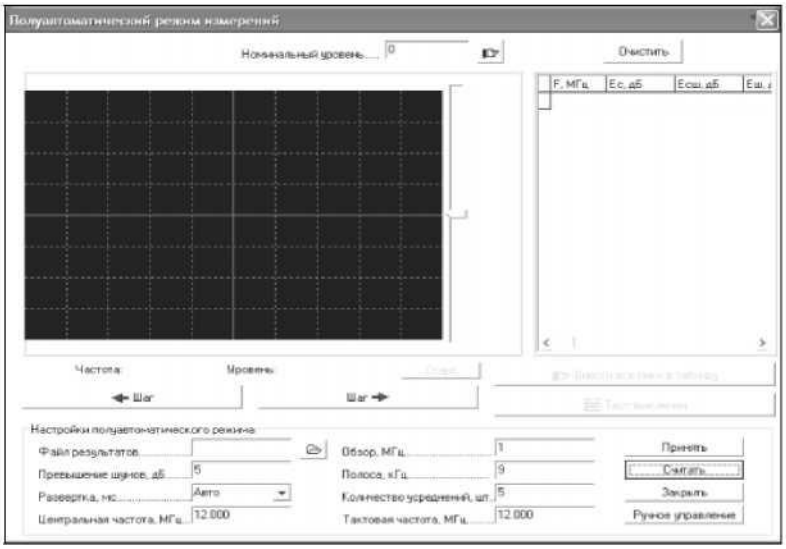


Рис. 2.1. Окно полуавтоматического режима

Нажмите кнопку «Принять». На дисплее окна полуавтоматического режима изображается текущее усреднение трека спектра. По завершении усреднений картинка останавливается.

Выключите тест на мониторе и нажмите «Тест выключен». На дисплее окна полуавтоматического режима отображаются в одной системе координат два графика частотного спектра (рис. 2.2): синим цветом с заполнением отображается график спектра при выключенном тесте, зеленым цветом - график спектра при включенном тесте. Белым цветом с заполнением показывается превышение шумов. Все видимые пики «зеленого» графика подлежат анализу как «подозрительные».

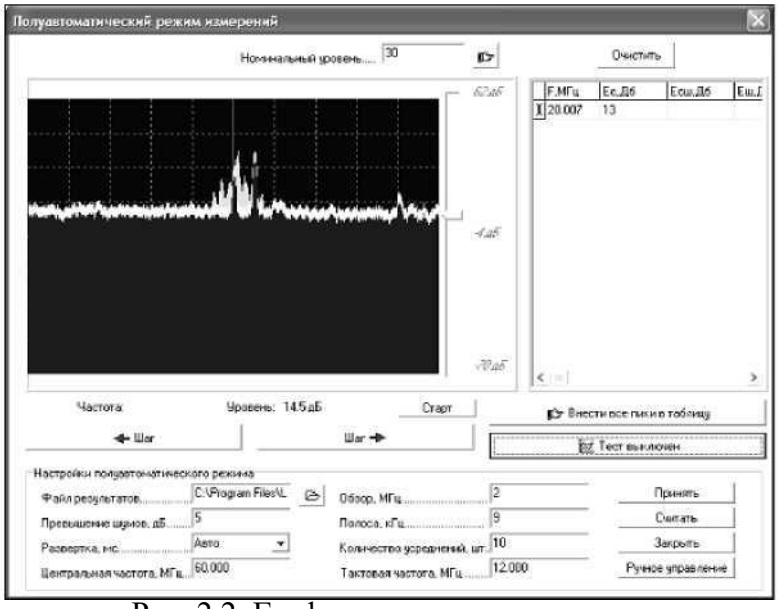


Рис. 2.2. Графики частотного спектра

Исследуйте все видимые пики «зеленого» графика. Для этого подведите курсор «мыши» к выбранному пику, удерживая нажатой левую кнопку «мыши». При этом внизу под дисплеем отображается значение частоты, совместно с курсором «мыши» перемещается маркер желтого цвета. Настроившись на нужный пик, отпустите левую кнопку «мыши». Поверх окна полуавтоматического режима выводится окно просмотра пика (рис. 2.3).

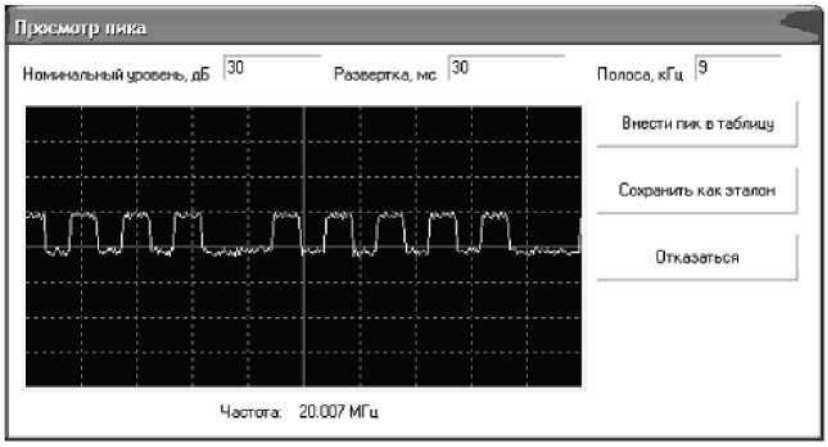


Рис. 2.3. Осциллограмма сигнала, демодулированного при помощи измерительного прибора

Включая и выключая тестовый режим работы исследуемого технического средства и наблюдая за осциллограммой, установите, принадлежит ли данное излучение гармоническим составляющим тестового сигнала. При обнаружении тестового сигнала

следует сохранить его как эталон, на жав на кнопку «Сохранить как эталон» окна просмотра пика. Сохраните в созданную папку со своим номером группы.

2.2.2. Контроль электромагнитной обстановки (ЭМО)

Выключите тест на исследуемом средстве;

Для предварительного контроля ЭМО следует составить программу исследования, для этого выберите в меню главного окна программы «Установки/Программа исследований». Поверх главного окна программы откроется окно параметров исследования на странице программы исследований (рис. 2.4).

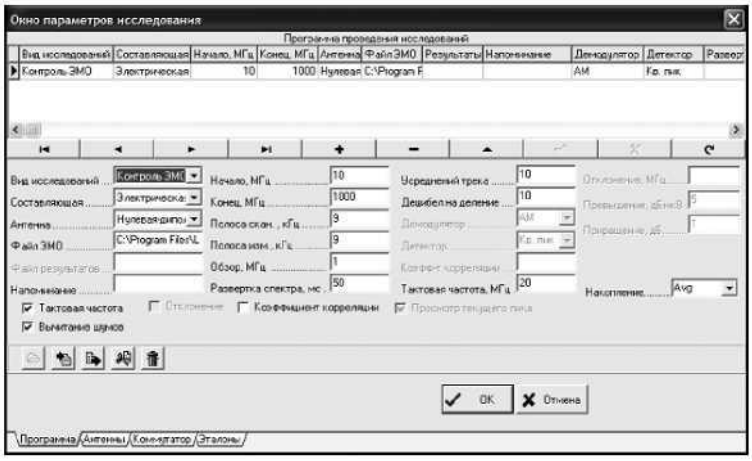


Рис. 2.4 . Окно параметров исследования

В таблице программы исследования, расположенной в верхней части страницы, отображается готовая к исполнению программа. По умолчанию таблица содержит программу, составленную при прошлом запуске управляющей программы. Сотрите старую программу нажатием кнопки «Мусорная корзина». Для экономии времени проведите контроль в окрестностях частот, кратных 20МГц (для монитора на ЭЛТ) или 60МГц.

После заполнения программы, внесите ее в таблицу нажатием кнопки «Внести в таблицу».

Нажмите кнопку «Ок». Программа автоматически сканирует выбранный диапазон и по завершении выдает сообщение «Программа исследования завершена». При этом, результаты сканирования сохранены в соответствующих выбранных файлах ЭМО для каждого диапазона и их можно использовать для автоматического поиска составляющих тестового сигнала при включенном тесте.

2.2.3. Автоматический поиск составляющих тестового сигнала Автоматический поиск гармонических составляющих тестового сигнала по заданному эталону можно производить методом беспропускового контроля по всему диапазону проведения спец-исследования, либо в окрестностях частот, кратных тактовой частоте теста. Для экономии времени проведите исследование в окрестностях частот, кратных 20МГц (для монитора на ЭЛТ) или 60МГц (для монитора на ЖК).

Для поиска составляющих тестового сигнала следует заполнить программу исследований. Для этого достаточно заменить вид исследований во всех заполненных строках таблицы на «Измерение ПЭМИН»;

После заполнения программы исследования загрузите эталон, найденный в полуавтоматическом режиме. Примерный вид эталона представлен на рис. 2.5.

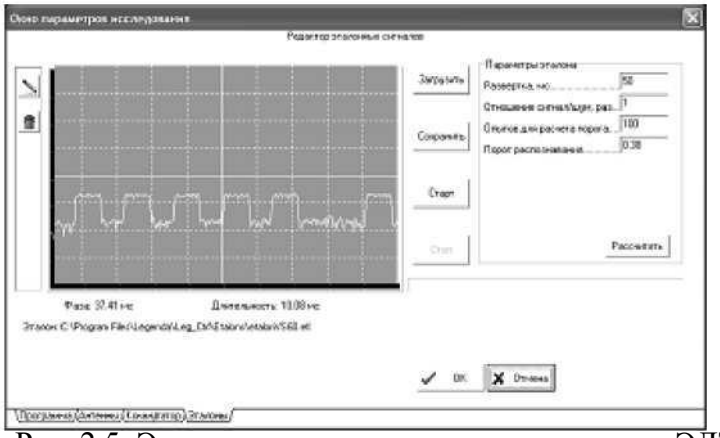


Рис. 2.5. Эталон тестового сигнала монитора на ЭЛТ

Рассчитайте пороговый коэффициент корреляции, нажав на кнопку «Рассчитать», после чего появится следующее окно (рис. 6).

Выберите в меню главного окна программы пункт «Измерения Старт», либо нажмите соответствующую кнопку быстрого запуска. Программа начнет сканировать диапазон, выделять пики, превышающие на заданное значение уровень шумов при выключенном тесте (если используется файл ЭМО).

Демодулированный сигнал будет сравниваться с эталоном и при превышении коэффициентом корреляции заданного порога, значение частоты будет занесено в таблицу. По завершении сканирования выдается сообщение «Выключите тест для измерения уровней шумов» и программа выполнит необходимые действия. В конце работы выдается сообщение «Программа исследований выполнена».

По завершении автоматического поиска и/или измерения ПЭМИН можно проконтролировать правильность обнаружения. Для этого щелкните «мышью» по любой строке таблицы обнаруженных частот главного окна управляющей программы.

На основном дисплее главного окна программы будет отображаться в реальном времени осциллограмма демодулированного сигнала на данной частоте. Включая и выключая тест на исследуемом техническом средстве и наблюдая за изменениями формы осциллограммы, можно сделать вывод о принадлежности данного излучения к составляющим тестового сигнала. В случае ложного срабатывания процедуры распознавания строку с ошибочно распознанным сигналом можно удалить, для чего следует нажать CTRL-DEL на клавиатуре управляющей ПЭВМ.

Рис. 2.6. Расчет порогового коэффициента корреляции

2.3. Расчет зон разведдоступности с помощью расчетной программы

2.3.1. Для запуска расчетной программы следует выбрать в меню «Пуск» соответствующий ярлык или вызвать исполняемый файл, на который ссылается данный ярлык («Легенда»).

2.3.2. Для того, чтобы загрузить данные измерений из файла в расчетную программу нужно выбрать в меню «Файл» пункт «Открыть». Появится стандартный диалог открытия файлов Windows. Далее пользователь должен указать файл, в котором содержатся данные измерений для расчета, полученные при работе управляющей программы, и нажать кнопку «Открыть». В случае правильной структуры файла в поля рабочей таблицы «F, МГц», «U, дБ» и «Цш, дБ» загрузятся значения частоты, уровня обнаруженных компонент тестового сигнала и уровня шума.

2.3.3. Для заполнения условий расчета следует выбрать в меню «Условия» команду «Заполнить». Пользуясь описанием процесса задания условий для расчета из предыдущей лабораторной работы, заполните условия, выставив отношение сигнал/шум для всех трех категорий 0,4.

2.3.4. После внесения и заполнения условий, нажмите Измерения-Старт. Программа рассчитает зоны разведдоступности.

2.3.5. После того, как программа выполнит расчет измерения, нужно сохранить результат в Microsoft Word с помощью кнопки быстрого доступа (документ Microsoft Word должен быть открыт).

Требования к отчету

Оформить отчет о проделанной работе.

В отчете привести: цель работы; задание на выполнение работы; порядок проведения работы; протоколы исследований в автоматическом и полуавтоматическом режимах. Сравнить результаты. Сделать выводы и ответить на контрольные вопросы.

Контрольные вопросы

1. Как решается проблема выделения информационных излучений?
2. Для чего необходим эталон тестового сигнала?
3. Каким образом происходит сравнение обнаруженного сигнала и образа эталонного сигнала?
4. Зачем необходим контроль ЭМО?
5. В каких режимах управляющая программа позволяет производить измерение ПЭМИН?

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1	1-2	1-3	1-3

Оценочные средства: ***отчет.***

Лабораторная работа № 13-14

Тема: Генераторы псевдослучайных последовательностей.

Цель работы:

- изучить статистические тесты, предложенные стандартом FIPS 140-1;
- изучить принципы формирования ПСЧ на основе линейного конгруэнтного генератора (ЛКГ) и линейного рекуррентного регистра (ЛРР);
- ознакомиться с примером практического использования ЛРР для формирования ПСП в системах мобильной связи.

Порядок выполнения работы

- ознакомится с представленным материалом;
- ответить на контрольные вопросы;
- оформить отчет.

1. Общие требования к генераторам ключевых данных

Безопасность любого криптоалгоритма определяется, в первую очередь, используемыми ключевыми данными. Ключевые данные должны отвечать определенной системе требований, зависящей как от типа криптопреобразований (симметричных или несимметричных), так и от специфических свойств используемого криптографического средства. Хотя ряд требований является общеприменимым (например, достаточная длина ключа, случайность, равновероятность и т.п.).

Рассмотрим кратко **основные свойства ЛРР и ЛРПМ** (на периоде).

1) Функционирование ЛРР (часто обозначают как $\langle \mathbf{m, f(x)} \rangle$) (существующие логические обратные связи) однозначно определяется используемым образующим полиномом $\mathbf{f(x)}$:

$$\mathbf{f(x) = c_m \cdot x^m + c_{m-1} \cdot x^{m-1} + \ldots + c_2 \cdot x^2 + c_1 \cdot x_1 + 1}, \quad \mathbf{f(x) \in Z_2[x]}, \qquad (2.1)$$

здесь $\mathbf{m}$ — старшая степень полинома;

$\mathbf{c_i}$ — численные коэффициенты ($\mathbf{c_i \in \{0, 1\}}$, $\mathbf{c_0 = 1}$).

2) Период ЛРПМ (линейной рекуррентной последовательности максимального периода) $\mathbf{T = 2^m - 1}$.

ЛРПМ может быть получена только при использовании примитивного образующего полинома $\mathbf{f(x)}$. В противном случае период формируемой последовательности будет заведомо меньшим.

3) Расстояние единственности равно $\mathbf{l_0 = 2 \cdot m}$ (где $\mathbf{m}$ — степень полинома).

То есть закон функционирования ЛРР (вид образующего полинома) может быть однозначно восстановлен по $\mathbf{2 \cdot m}$ безошибочно полученным подряд расположенным символам. Это и следующее (связанное с ним) свойство являются основными недостатками ЛРР, из – за которых они не могут использоваться в изолированном виде в качестве ГКП.

4) Структурная скрытность $\mathbf{S_c = l_0 / T = 2 \cdot m / (2^{m-1})}$.

То есть структурная скрытность для ЛРР достаточно низкая — закон функционирования ЛРР легко раскрываем.

5) Количество нулей (на периоде ЛРПМ) на один меньше количества единиц: $\mathbf{2^{m-1} - 1}$ и $\mathbf{2^{m-1}}$ соответственно.

6) Длина максимальной серии из единиц — $\mathbf{m}$, из нулей — $\mathbf{(m - 1)}$.

7) Свойства псевдослучайности: из общего количества серий на периоде ЛРПМ

$\mathbf{1/2}$ всех длин имеют длину $\mathbf{1}$;

$\mathbf{1/4}$ — длину $\mathbf{2}$;

. . .

$\mathbf{1/2^k}$ — длину $\mathbf{k}$.

8) На периоде ЛРПМ по одному разу встречаются все $\mathbf{m}$ – разрядные комбинации от $\mathbf{1}$ до $\mathbf{2^m - 1}$ (свойство “окна”).

9) Количество изоморфизмов ЛРПМ $\mathbf{N_И = \varphi(T) / m}$ (здесь $\mathbf{\varphi(T)}$ — значение функции Эйлера).

То есть для данной степени $\mathbf{m}$ существует $\mathbf{N_И}$ примитивных полиномов и, соответственно, $\mathbf{N_И}$ ЛРПМ, отличающихся тонкой структурой и не являющихся циклическими сдвигами друг относительно друга (см. табл. Б.1).

10) Сумма двух ЛРПМ, отличающихся только циклическим сдвигом, также является ЛРПМ, отличающейся от двух исходных только циклическим сдвигом.

То есть комбинирование (линейное) нескольких отрезков одной и той же ЛРПМ не дает увеличения структурной скрытности.

В качестве начального содержимого регистра — битов $\{S_{m-1}, S_{m-2}, \ldots, S_1, S_0\}$ — задается случайный (псевдослучайный) двоичный **m** – разрядный вектор (запрещенной является только нулевая комбинация).

Бит обратной связи ЛРР (в соответствии с (2.1)) формируется согласно следующему соотношению:

$$c_0 \cdot S_j = \bigoplus_{k=1}^{m} c_k \cdot S_{j-k}\ ,\ j \geq m,$$

где S_j — содержимое ячеек регистра;

c_i — коэффициенты образующего полинома (причем $c_0 = 1$).

2.Статистические тесты для генераторов случайных чисел, описанные в стандартах FIPS 140 - 1 и FIPS 140 - 2

Рассматриваемый стандарт FIPS 140 – 1 [**Ошибка! Источник ссылки не найден.**] рекомендует для оперативного тестирования последовательностей, формируемых некоторым ГПСП (генератором псевдослучайных последовательностей) использовать 4 теста. При этом для проведения тестирования требуется битовая строка длиной 20 тыс. бит. При этой длине исследуемой последовательности допустимые интервалы для статистик, вычисляемых по каждому из тестов, задаются в явном виде (то есть нет необходимости предварительно выбирать соответствующие уровни значимости). Рассмотрим кратко предлагаемые стандартом тесты.

В стандарте FIPS 140 – 2 [**Ошибка! Источник ссылки не найден.**, **Ошибка! Источник ссылки не найден.**] для уменьшения вероятности принятия ошибочного решения были пересмотрены (сделаны более жесткими) допустимые интервалы для каждого из статистических тестов.

Монобитный тест (частотный тест).

В исследуемой последовательности количество единичных бит N_1 (и количество нулевых бит N_0) должно находиться в следующем интервале.

FIPS 140 - 1	$9\,654 < N_1 < 10\,346$
FIPS 140 - 2	$9\,725 < N_1 < 10\,275$

Покер – тест (блочный тест).

По исследуемой последовательности подсчитывается следующая статистика:

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k\ ,$$

где **m** —длина подсчитываемых неперекрывающихся подпоследовательностей (для данного стандарта принято **m = 4**);

n_i —количество появлений подпоследовательности **i** – того типа длины **m** (для **m = 4** существует $2^m = 2^4 = 16$ типов подпоследовательностей);

k —общее количество неперекрывающихся подпоследовательностей длины **m** (для данного стандарта **k = 20 000 / 4 = 5 000**).

Значение полученной статистики X_3 должно находиться в следующем интервале.

FIPS 140 - 1	$1.03 < X_3 < 57.4$
FIPS 140 - 2	$2.16 < X_3 < 46.17$

Тест серий.

Серией считают подпоследовательность исходной последовательности, которая состоит из битов одного типа (либо '0', либо '1'), которым не предшествует и за которыми не следует бит того же типа ('0' или '1' соответственно).

В данном тесте для исследуемой последовательности подсчитывается количество единичных S_i и количество нулевых Z_i серий длины **i** ($1 \leq i \leq 6$, серии большей длины в данном тесте рассматриваются как серии длины **6**).

Тест серий считается успешно пройденным, если все **12** подсчитанных значения (S_i и Z_i, $1 \leq i \leq 6$) принадлежат соответствующим интервалам, приведенным в следующей таблице.

Длина серии		1	2	3	4	5	≥ 6
Допустимые диапазоны	FIPS 140-1	2 267 – 2 733	1 079 – 1 421	502 - 748	223 - 402	90 - 223	90 - 223
	FIPS 140-2	2 343 – 2 657	1 135 – 1 365	542 - 708	251 - 373	111 - 201	111 - 201

Тест максимальной длины серии.

Тест считается успешно пройденным, если в исследуемой последовательности не существует серий длиной **34** и более.

Если хотя бы один из рассмотренных тестов терпит неудачу, то исследуемая последовательность (а следовательно, и сформировавший ее ГПСП) не проходит тестирование. Стандарт рекомендует в криптографических приложениях с высокими требованиями к уровню безопасности выполнять эти тесты при каждом запуске генератора случайных (псевдослучайных) бит.

Стандарт FIPS 140 – 1 допускает возможность замены вышеописанных тестов альтернативными вариантами, обеспечивающими эквивалентное (или лучшее) качество проверки случайности.

Лабораторная работа № 15-16

Тема: Линейный конгруэнтный и рекуррентный генераторы ПСП.

Цель работы:

- изучить статистические тесты, предложенные стандартом FIPS 140-1;
- изучить принципы формирования ПСЧ на основе линейного конгруэнтного генератора (ЛКГ) и линейного рекуррентного регистра (ЛРР);
- ознакомиться с примером практического использования ЛРР для формирования ПСП в системах мобильной связи.

Порядок выполнения работы

- ознакомится с представленным материалом;
- ответить на контрольные вопросы;
- оформить отчет.

Линейный конгруэнтный генератор.

Линейный конгруэнтный генератор формирует последовательность чисел согласно выражению

$$x_{i+1}=(a\,x_i+c)\bmod m,$$

где a, c и m - целочисленные коэффициенты.

Длина периода линейной конгруэнтной последовательности зависит от выбора коэффициентов a, c и m. Длина периода равняется m тогда, когда

- c и m есть взаимно простыми числами;
- b = a-1 кратно числу p для любого простого p, которое есть делителем m;
- b кратно 4, если m кратно 4.

Коэффициент c может равняется 0. В этом случае получим мультипликативный датчик

$$x_{i+1} = a\,x_i \bmod m.$$

Максимально возможный период при c = 0 равняется $\lambda(m)$, где

$$\lambda(2^e) = 2^{e-2};$$
$$\lambda(p^e) = p^{e-1}(p-1);$$

Такой период будет получен, если:

- x_0 и m взаимно простые числа;
- a – первообразный элемент по модулю m.

При выполнении лабораторных работ можно использовать следующие параметры для ЛКГ (табл.1), или самостоятельно сформировать необходимые параметры. Описание ЛГК в таблице 1 дано в такой последовательности LCG(m, a, c, x_0).

Таблица 1.

Имя	Описание
RANDU	LCG (2^{31}, 65539,0,1)
MINSTD	LCG(2^{31}-1, 16807,0,1)
MINSTD-25	LCG(2^{31}-1, 1817129560,0,1)
ANSIC	LCG(2^{31}-1, 1103515245,12345,12345)
ANSIC-25	LCG(2^{31}-1, 788950093,2103497953,12345)
ANSIC-203	LCG(2^{31}-1, 1471780181,1584727831,12345)
Short SIM1	LCG(2^{30}, 74125,227623267,1)
Short SIM2	LCG(2^{30}, 982525,227623267,1)
Fisman LCG's	LCG(2^{31}-1, a, 0, 1) a = {599496926, 742938285, 950706376, 1226874159, 62089911, 1343714438}

SIMSCRIPT	LCG(2^{31}-1, 630360016,0,1)
URN12	LCG(2^{31}, 452807053,0,1)
Hoaling LCG's	LCG(2^{31}-1, a, 0, 1) a = {107831381, 1203248318, 397204094, 2027812808, 1323257245, 764261123}
L'Ecuer LCG's	LCG(2^{31}-1, a, 0, 1) a = {1385320287, 41358138532028713853202 87}

Получения выборки псевдослучайных чисел с помощью ЛКГ

Запустите программу **CLinCongGener.exe**.

- В поле “Путь к файлу с выборкой” укажите файл, где должна быть сохраненная выборка (возможная включения полного или относительного пути в имени файла). Если файл уже существует, его содержимое будет заменено новой выборкой случайных чисел. Если указанного файла нет, он будет создан. Нажав на кнопку “Выбрать...” или избрав пункт меню Файл/Выбрать файл..., Вы можете задать имя с помощью стандартного диалога Windows для выбора файла.
- В поле “Размер выборки” укажите размер выборки в байтах (2500).
- В полях “Параметры ЛКГ” задайте параметры генератора: множитель a, начальное состояние x_0, перенос c , модуль m (десятичные числа, которые находятся в диапазоне от 1 до 2^{32}-1= 4294967295).
- Нажмите кнопку “Запуск”.

После выполнения указанных действий начнется генерация выборки. Для сообщения пользователю о ходе генерации будет выведенное окно индикации, в котором графически отображается уже сформированная часть выборки. Под индикатором находится кнопка “Прервать”, нажав на которую, можно корректно прервать генерацию после соответствующего подтверждения. Если генерация была прервана, файл с уже сформированной частью выборки будет удален.

Интерфейс утилиты разрешает сохранять размер выборки, путь и имя файла с выборкой, язык интерфейса и параметры линейного конгруэнтного генератора, используемые в текущем сеансе работы. Если вы хотите, чтобы эти параметры были доступные в следующем сеансе работы, убедитесь, что в меню Настройка/Сохранить отмеченный соответствующий параметр.

Для окончания работы с утилитой нажмите кнопку “Выход” или выберите пункт меню Файл/Выход. При этом отмеченные в меню Настройка/Сохранить параметры будут сохраненные и загружены в следующем сеансе работы.

Линейный рекуррентный регистр (ЛРР).

ЛРР в особенности часто используют для получения псевдослучайных последовательностей. ЛРР простое в реализации, недорогое устройство, способное формировать последовательности и обеспечить такие требования как:

- большой размер ансамбля последовательностей, формируемых на одной алгоритмической основе;
- оптимальность корреляционных функций в ансамбле;
- сбалансированность структуры;
- максимальность периода для данной длины регистра сдвига.

ЛРР представляет собой регистр сдвига с обратными связями, объединенными по модулю 2. Его структурная схема представлена на рисунке 1.

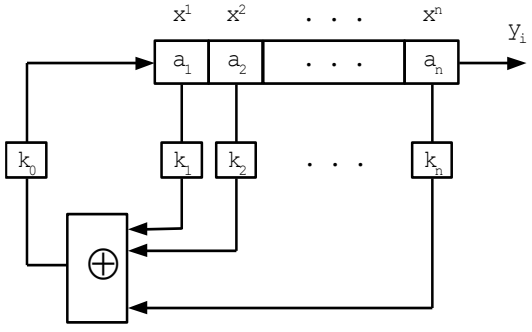


Рисунок 1. Структурная схема ЛРР

Очередное значение, которое формируются на выходе ЛРР, исчисляется по формуле

$$a_{n+1} = \bigoplus_{j=0}^{n} a_j h_j ,$$

где $\oplus$ - операция вычисления суммы за модулем 2,

a_j - состояние j -го биту ЛРР

h_j - коэффициент обратной связи.

При этом для двоичного ЛРР $a_j, h_j \in \{0,1\}$.

Каждому линейному рекуррентному регистру длиной n разрядов можно сопоставить полином обратных связей h(x) с двоичными коэффициентами вида

$$h(x) = h_n x^n + h_{n-1} x^{n-1} + \ldots + h_1 x + h_0 ,$$

причем обязательно $h_n = h_0 = 1$.

Если полином h(x) - примитивный, то длина последовательности, которая генерируется ЛРР, максимальная и равняется

$$L_{\max} = 2^n - 1.$$

Необходимо учитывать, что в чистом виде линейные рекуррентные последовательности не используются из-за низкой структурной скрытности сформированных последовательностей. Для повышения структурной скрытности используют:

- комбинирования нескольких ЛРР;
- нелинейные функции в обратной связи регистра;
- нелинейную логику и фильтрацию содержимого регистра.

В качестве полинома для лабораторных работ рекомендуется использовать следующие полиномы

Таблица 2

$x^{20} + x^3 + 1$	$x^{41} + x^{20} + 1$
$x^{20} + x^5 + 1$	$x^{41} + x^3 + 1$
$x^{31} + x^3 + 1$	$x^{52} + x^7 + 1$
$x^{31} + x^{13} + 1$	$x^{52} + x^{21} + 1$

Получения псевдослучайных чисел из линейного рекуррентного регистра

Запустите программу **CLRRGener.exe**. В окне “Генератор на ЛРР” задайте следующие параметры:

- В поле “Путь к файлу с выборкой” укажите файл, где должна быть сохраненная выборка. Если файл уже существует, его содержание будет заменено новой выборкой. Если указанного файла нет, он будет создан. Нажав кнопку “Выбрать…”или избрав пункт меню Файл/Выбрать файл…,Вы можете задавать имя с помощью стандартного диалога Windows для выбора файла.
- В группе параметры полинома (тринома) ЛРР задайте в полях “n1” и “n2” его коэффициенты n1 и n2 (коэффициенты должны находиться в границах от 3 до 999 степени). Потом выберите начальное заполнение ЛРР: всеми единицами отметив поле “Все единицы”, одной единицей в младшем разряде и других нулях, отметив поле “Одна единица, все нули” или случайное, отметив поле “Случайное”.
- В поле “Размер выборки” укажите размер выборки в байтах (2500). Генерация больших выборок может занять значительное время.
- Нажмите кнопку “Запуск”.

После выполнения указанных действий начнется генерация выборки. Для сообщения пользователя о ходу генерации будет выведенное окно индикации, в котором графически отображается уже сформированная часть выборки. Под индикатором находится кнопка прервать, нажав которое, можно корректно прервать генерацию после соответствующего подтверждения. Если генерация была прервана, файл выборки не будет создан.

Для окончания работы с утилитой нажмите кнопку “Выход” или изберите пункт меню Файл/Выход.

Архиваторы как источник псевдослучайных чисел.

В лабораторных работах, для сравнения результатов, как источник псевдослучайных чисел можно использовать программы сжатия: ARJ, RAR, ZIP и др. Принцип работы архиваторов основан на удалении избыточности. В общем случае на выходе архиватора формируется безизбыточный файл с хорошими статистическими свойствами.

В лабораторных работах можно формировать файлы данных путем сжатия любых других файлов архиватором. Как исходные файлы можно также использовать файлы данных, полученных с использованием аппаратных генераторов, ЛКГ и ЛРР.

Схемы поточного шифрования используются во многих практических приложениях. Например, в системах мобильной связи стандарта GSM алгоритм шифрования речи A5 использует сложение по модулю 2 данных (после соответствующего преобразования речи в двоичную последовательность) и ПСП (псевдослучайная последовательность), которая вырабатывается тремя ЛЛР с псевдослучайным тактированием. В лабораторной работе подобной схемой является генератор ПСП со сжатием.

На приемной стороне ПСП (гамма) снимается повторным сложением по модулю 2 с поступающим на вход цифровым потоком.

Пример практически используемого в стандарте GSM потокового шифра A5/1

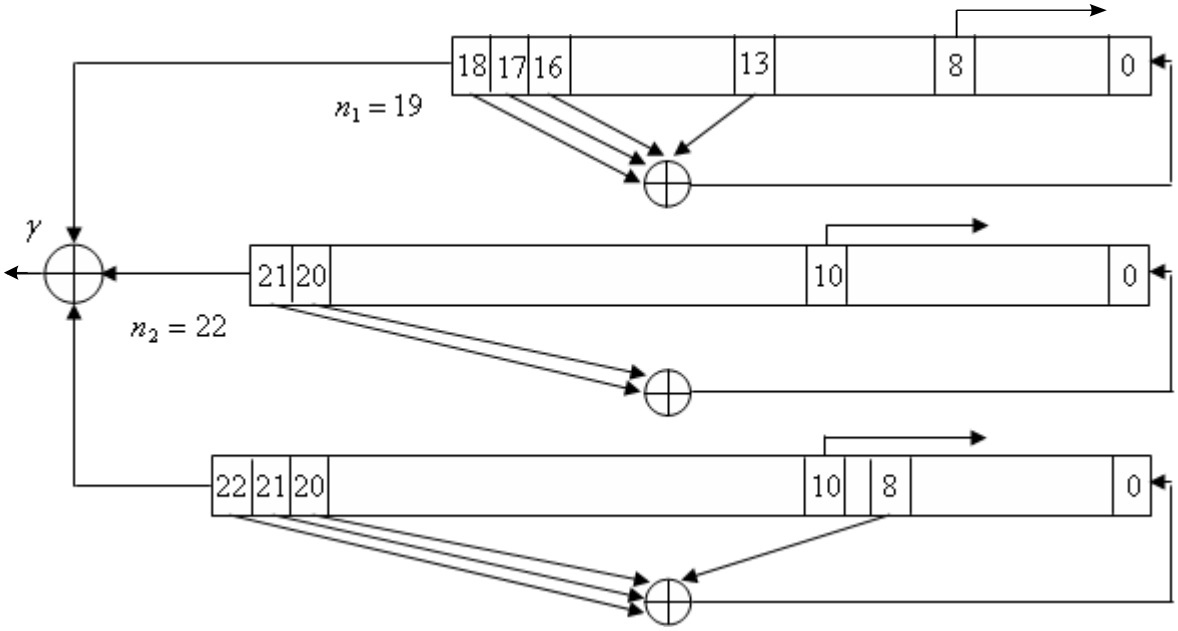


Рисунок 2. Алгоритм шифрования A5/1 стандарта GSM

Из рис.2 видно, что генератор гаммы потокового шифра A5/1 состоит из трех ЛРР длины 19, 22 и 23 с отводами обратных связей, соответствующих примитивным полиномам, показанным на рисунке **($x^{18}+x^{17}+x^{16}+x^{13}+x^8+1$; $x^{21}+x^{20}+x^{10}+1$; $x^{22}+x^{21}+x^{20}+x^{10}+x^8+1$).** Это обеспечивает периоды выходных последовательностей данных ЛРР, равные соответственно $2^{19}-1, 2^{22}-1, 2^{23}-1$.

Все три регистра используют псевдослучайное тактирование, которое работает по следующему правилу: биты с отвода 8 первого ЛРР, а также с отводов 10 второго и третьего ЛРР, подаются на так называемый мажоритарный элемент. Последний выдает на выходе значение 0 или 1, в зависимости от того, появляется ли на его входах больше нулей или единиц. Далее выход этого мажоритарного элемента сравнивается со значениями выходов на трех отводах ЛРР с номерами 8, 10, 10 (которые подавались ранее на входы этого мажоритарного элемента), и каждый ЛРР продвигается на один такт тогда и только тогда, когда сравниваемые биты оказываются одинаковыми. Шифрующая гамма формируется как сумма по модулю 2 выходов всех трех ЛРР. Ключом являются начальные заполнения всех ЛРР, которые вводятся на начальном этапе без псевдослучайного тактирования.

Длина ключа оказывается , таким образом равной 19+22+23=64 бита.

Стойкость шифра A5/1

При разработке этого шифра предполагалось, что он будет иметь высокую стойкость, так как количество его ключей достаточно велико, однако дальнейшие исследования, проводившиеся независимыми криптографами [ ] показали, что у этого шифра есть слабые стороны. Одна из них состоит в том, что ЛРР, входящие в состав шифратора имеют малые длины, и поэтому они подвержены некоторым модификациям статистических атак, а также атакам на основе обменных соотношений между требуемым объемом памяти и временем анализа.

В конечном итоге, исследования, которые проводились начиная с 2000 года (то есть почти сразу же после введения этого стандарта), показали, что данный шифр может быть “взломан” с использованием

обычного ПК в реальном времени. Результаты этих исследований для различных типов атак помещены в Таблице 1.

Типы атак	Время предварительной обработки	Время приема гаммы	Количество 73 Gb дисков	Время вскрытия шифра
1	2^{42} тактов	2 мин	4	1 сек
2	2^{48} тактов	2 мин	2	1 сек
3	2^{48} тактов	2 сек	4	1 мин

Таблица 1. Криптоанализ шифра A5/1.

Как видно из данной таблицы, шифр A5/1 не обладает высокой стойкостью, даже если он подвергается атакам со стороны непрофессиональных криптографов, имеющих в своем распоряжении лишь персональные компьютеры.

Контрольные вопросы.

1. Объясните процесс формирования псевдослучайных чисел с использованием ЛКГ.
2. Объясните процесс формирования псевдослучайной последовательности с использованием ЛРР.
3. Поясните суть монобитного теста.
4. Поясните суть блочного теста.
5. Поясните суть теста серий.
6. Поясните суть теста длин серий.
7. Объясните процесс отбора псевдослучайных последовательностей по Fips-140.
8. Общие требования к генераторам ключевых данных
9. Объясните процесс работы потокового шифра A5/1.

Лабораторная работа № 17-18. «Контроль эффективности защиты речевой информации»

Цель работы:

Целью данной лабораторной работы является разборчивость речи полученной при перехвате информации средствами разведки по прямому акустическому или виброакустическому каналам.

1. Теоретическая часть

1.1. Разборчивость речи при перехвате информации средствами разведки по прямому акустическому и виброакустическому каналам.

Защита акустической (речевой) информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта или учреждения.

Для перехвата речевой информации предполагаемый "противник" (лицо или группа лиц, заинтересованных в получении данной информации) может использовать широкий арсенал портативных средств акустической речевой разведки, позволяющих перехватывать речевую информацию по прямому акустическому, виброакустическому, электроакустическому и оптико-электронному (акустооптическому) каналам, к основным из которых относятся:

- портативная аппаратура звукозаписи (малогабаритные диктофоны, магнитофоны и устройства записи на основе цифровой схемотехники);
- направленные микрофоны;
- электронные стетоскопы;
- электронные устройства перехвата речевой информации (закладные устройства) с датчиками микрофонного и контактного типов с передачей перехваченной информации по радио, оптическому (в инфракрасном диапазоне длин волн) и ультразвуковому каналам, сети электропитания, телефонным линиям связи, соединительным линиям вспомогательных технических средств или специально проложенным линиям;
- оптико-электронные акустические системы и т.д.

Портативная аппаратура звукозаписи и закладные устройства с датчиками микрофонного типа (преобразователями акустических сигналов, распространяющихся в воздушной и газовой средах) могут быть установлены при неконтролируемом пребывании физических лиц ("агентов") непосредственно в выделенных (защищаемых) помещениях. Данная аппаратура обеспечивает регистрацию речи средней громкости при удалении микрофона на расстоянии до 15.. .20 м от источника речи.

Электронные стетоскопы и закладные устройства с датчиками контактного типа позволяют перехватывать речевую информацию без физического доступа "агентов" в выделенные помещения. При этом датчики закладных устройств наиболее часто устанавливаются вблизи мест возможной утечки речевой информации: микрофонного типа - в выходах кондиционеров и каналах систем вентиляции; контактного типа (преобразователи виброакустических сигналов, распространяющихся по строительным конструкциям зданий, инженерным коммуникациям и т.п.) - на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем. Экспериментальные исследования показали, что с использованием данных средств разведки обеспечивается перехват речевой информации с высоким качеством через ограждающие конструкции в железобетонных зданиях через 1.2 этажа, по трубопроводам через 2.3 этажа и по вентиляционным каналам на расстоянии до 20.30 м.

Применение для ведения разведки направленных микрофонов и оптико-электронных (лазерных) акустических систем не требует проникновения "агентов" не только в выделенные и смежные с ними помещения, но и на охраняемую территорию объекта. Разведка может вестись из соседних зданий или автомашин, находящихся на автостоянках, прилегающих к зданию.

С использованием направленных микрофонов возможен перехват речевой информации из выделенных помещений при наличии открытых оконных проемов (форточек или фрамуг) в условиях города (на фоне транспортных шумов) на расстояниях до 50 м. За городом при оптимальных условиях дальность разведки может составлять до 80.. .100 м днем и до 200 м в ночное время.

Максимальная дальность разведки с использованием оптико-электронных (лазерных) акустических систем, снимающих информацию с внутренних стекол, составляет 150.200 метров в городских условиях (наличие интенсивных акустических помех, запыленность атмосферы) и до 500 м в загородных условиях.

Защита акустической (речевой) информации достигается проектноархитектурными решениями, проведением организационных и технических мероприятий, а также выявлением электронных устройств перехвата информации.

Использование тех или иных методов и средств определяется характеристиками объекта защиты и аппаратуры разведки, условиями ее ведения, а также требованиями, предъявляемыми к эффективности защиты акустической (речевой) информации, в качестве показателя оценки которой наиболее часто используют словесную разборчивость W.

Критерии эффективности защиты акустической (речевой) информации во многом зависят от целей, преследуемых при организации защиты, например:

- скрыть смысловое содержание ведущегося разговора;
- скрыть тематику ведущегося разговора и т.д.

Процесс восприятия речи в шуме сопровождается потерями составных элементов речевого сообщения. Понятность речевого сообщения характеризуется количеством правильно принятых слов, отражающих качественную область понятности, которая выражена в категориях подробности справки о перехваченном разговоре, составляемой "агентом".

Проведенный анализ показал возможность ранжирования понятности перехваченного речевого сообщения. Из практических соображений может быть установлена некоторая шкала оценок качества перехваченного речевого сообщения:

- Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное для составления подробной справки о содержании перехваченного разговора.
- Перехваченное речевое сообщение содержит количество правильно понятых слов, достаточное только для составления краткой справки-аннотации, отражающей предмет, проблему, цель и общий смысл перехваченного разговора.
- Перехваченное речевое сообщение содержит отдельные правильно понятые слова, позволяющие установить предмет разговора.
- При прослушивании фонограммы перехваченного речевого сообщения возможно установить факт наличия речи, но нельзя установить предмет разговора.

В соответствии с ГОСТ Р 50840-95 понимание передаваемой речи с большим напряжением внимания, переспросами и повторениями наблюдается при слоговой разборчивости 25 - 40 %, а при слоговой разборчивости менее 25 % имеет место неразборчивость связного текста (срыв связи) на протяжении длительных интервалов времени [3]. Учитывая взаимосвязь словесной и слоговой разборчивости [4], можно рассчитать, что срыв связи будет наблюдаться при словесной разборчивости менее 71%.

Практический опыт показывает, что составление подробной справки о содержании перехваченного разговора невозможно при словесной разборчивости менее 60 - 70 %, а

краткой справки-аннотации - при словесной разборчивости менее 40 - 50 %. При словесной разборчивости менее 20 - 30 % значительно затруднено установление даже предмета ведущегося разговора, а при словесной разборчивости менее 10 % это практически невозможно даже при использовании современной техники фильтрации помех.

Проведенные многочисленные измерения и расчеты показали, что без применения специальных методов и средств защиты акустической (речевой) информации качество перехватываемых средствами акустической разведки сообщений вполне достаточно для составления подробной справки о содержании перехваченного разговора.

Для снижения разборчивости речи необходимо стремиться уменьшить отношение "уровень речевого сигнала/уровень шума" (сигнал/шум) в местах возможного размещения датчиков аппаратуры акустической разведки. Уменьшение отношения сигнал/шум возможно путем или уменьшения (ослабления) уровня речевого сигнала ***(пассивные методы защиты),*** или увеличения уровня шума (создания акустических и вибрационных помех) ***(активные методы защиты).***

1.2. Ослабление акустических (речевых) сигналов. Звукоизоляция строительных конструкций. Звукоизоляция оконных рам. Активные методы защиты.

Ослабление акустических (речевых) сигналов осуществляется путем звукоизоляции помещений, которая направлена на локализацию источников акустических сигналов внутри них.

Звукоизоляция оценивается величиной ослабления акустического сигнала и обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделочных материалов.

В случае если звукоизоляция помещения не обеспечивает требуемой эффективности защиты информации, то для ее повышения используют специальные звукопоглощающие материалы.

Наиболее часто применяют облицовочные звукопоглощающие материалы в виде плоских плит (плиты "Акмигран", "Акмант", "Силаклор", "Винипор", ПА/С, ПА/О, ПП-80, ППМ, ПММ), располагаемые или вплотную, или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т.п.). Используются также звукопоглощающие облицовки из слоя пористо-волокнистого материала (стеклянного или базальтового волокна, минеральной ваты) в защитной оболочке из ткани или пленки с перфорированным покрытием (металлическим, гипсовым и др.).

Повышение звукоизоляции стен и перегородок помещений также достигается установкой на расстоянии в 6.. .10 см от них однослойных и многослойных (чаще двойных) ограждений. В многослойных ограждениях целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например, бетон - поролон).

Для снижения величины вибрационного сигнала используются мягкие прокладки (виброизолирующие опоры), которыми развязываются друг от друга различные ограждающие конструкции. В качестве таких прокладок применяют твердую резину, пробку, свинец.

При звукопоглощающей отделке внутреннего пространства помещений можно добиться повышения звукоизоляции на 10.15 дБ, что в большинстве случаев оказывается достаточным для обеспечения требований по защите.

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т.д.). Для них в стенах и перекрытиях сооружений делают соответствующие отверстия и проемы, что значительно снижает звукоизоляцию помещений в целом.

Звукоизоляция отверстий и проемов обеспечивается применением специальных гильз, коробов, прокладок, глушителей, вязкоупругих заполнителей и т.д.

Развязка трубопроводов достигается установкой в разрыв трубы специальных резиновых вставок, которые могут выдерживать давление воды теплоцентрали. При этом сама труба должна быть виброразвязана от конструкции стен и перегородок, через которые она проходит.

Система приточно-вытяжной вентиляции и воздухообмена зон выделенных помещений не должна быть связана с системой вентиляции других помещений и иметь свой отдельный забор и выброс воздуха. Вентиляционные камеры забора и выброса рекомендуется располагать на крыше здания, а сами вентиляционные отверстия не должны выходить в места возможного дистанционного контроля. В случае невозможности выполнения этого требования рекомендуется на вводах и выходах каналов вентиляционных систем в зону выделенных помещений устанавливать акустические фильтры и глушители звука, а в разрыв воздуховода - мягкие вставки из плотной ткани или резины.

Одним из наиболее слабых звукоизолирующих элементов ограждающих конструкций выделенных помещений являются двери и окна.

Звукопоглощающая способность окон зависит, главным образом, от поверхностной плотности стекла и степени прижатия притворов.

Звукоизоляция окон с одинарным остеклением не обеспечивает требуемой эффективности защиты информации. Обычные окна с двойными переплетами обладают более высокой (на 4...5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон. Повышение звукоизоляции до 5 дБ наблюдается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием.

Существенное повышение звукоизоляции в сравнении с обычным окном дают оконные блоки специальной конструкции. Такие блоки выполняются из комбинаций 4...7 мм стекол, установленных на расстоянии не менее 200 мм (по крайней мере, двух из них), и имеют высококачественный притвор из уплотняющей резины, что в совокупности обеспечивает звукоизоляцию 40.45 дБ.

Стандартные одинарные двери не могут обеспечить требования на звукоизоляцию, даже если выполнены требования на плотность и тщательность исполнения и подгонки дверного полотна к дверной коробке и устранены щели между дверью и полом.

Увеличение звукоизолирующей способности дверей достигается применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д.

Для защиты информации в особо важных помещениях используются двери со звукоизолирующим дверным проемом, выполненном в виде тамбура с глубиной не менее 0,5 м. При этом внутреннее пространство тамбура должно быть отделано звукопоглощающим материалом, притворы дверей оборудованы уплотнителями, а двери обиты звукопоглотителем на обивочном материале.

В особо важных помещениях используют специальные звукоизолирующие двери.

Пассивные методы защиты информации, как правило, реализуются при строительстве или реконструкции зданий на этапе разработки проектных решений, что позволяет заранее учесть типы строительных конструкций, способы прокладки коммуникаций, оптимальные места размещения выделенных помещений.

В случае технической невозможности использования пассивных средств защиты помещений или если они не обеспечивают требуемых норм по звукоизоляции, используются активные меры защиты.

1.3. Активные методы защиты

Активные методы защиты заключаются в создании маскирующих акустических и вибрационных помех средствам разведки, то есть использованием виброакустической маскировки информационных сигналов.

Акустическая маскировка эффективно используется для защиты речевой информации от утечки по всем каналам утечки, а виброакустическая - по виброакустическому и оптико-электронному (акустооптическому) каналам.

В настоящее время создано большое количество различных систем активной виброакустической маскировки, успешно используемых для подавления средств перехвата речевой информации. К ним относятся: системы "Заслон", "Кабинет", "Барон", "Порог-2М", "Фон-В", "Шорох", VNG-006, ANG-2000, NG-101, "Эхо" и т.д. .

Для формирования виброакустических помех применяются специальные генераторы на основе электровакуумных, газоразрядных и полупроводниковых радиоэлементов. На практике наиболее широкое применение нашли генераторы шумовых колебаний.

Наряду с шумовыми помехами в целях активной акустической маскировки используют "речеподобные" помехи, хаотические последовательности импульсов и т.д.

Роль оконечных устройств, осуществляющих преобразование электрических колебаний в акустические колебания речевого диапазона частот, обычно выполняют малогабаритные широкополосные акустические колонки, а осуществляющих преобразование электрических колебаний в вибрационные - вибрационные излучатели.

Акустические колонки систем зашумления устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки, а вибрационные излучатели крепятся на оконных рамах, стеклах, коробах, трубопроводах, стенах, потолках и т.д.

В состав типовой системы виброакустической маскировки входят шумогенератор и от 6 до 12...25 вибрационных излучателей (пьезокерамических или электромагнитных). Дополнительно в состав системы могут включаться звуковые колонки.

Для полной защиты помещения по виброакустическому каналу вибродатчики должны устанавливаться на всех ограждающих конструкциях (стенах, потолке, полу), оконных стеклах, а также трубах, проходящих через помещение. Требуемое количество вибродатчиков для защиты помещения определяется не только его площадью, количеством окон и труб, проходящих через него, но и эффективностью датчиков (эффективный радиус действия вибродатчиков на перекрытии толщиной 0,25 м составляет от 1,5 до 5 м) [10].

Защита нескольких помещений маскирующим шумом от одного генератора нецелесообразна, поскольку реальной становится опасность эффективного применения многоканальной компенсации шума.

При организации акустической маскировки необходимо помнить, что акустический шум может создавать дополнительный мешающий для сотрудников фактор (дискомфорт) и раздражающе воздействовать на нервную систему человека, вызывая различные функциональные отклонения, приводить к быстрой утомляемости работающих в помещении. Степень влияния мешающих помех определяется санитарными нормативами на величину акустического шума. В соответствии с нормами для учреждений величина мешающего шума не должна превышать суммарный уровень 45 дБ.

Учитывая, что для выполнения требуемых норм по защите речевой информации необходимо создание на различных элементах и конструкциях (оконных рамах, стеклах, коробах, трубопроводах, стенах, потолках и т.д.) различных уровней помеховых сигналов, требуется создание многоканальных систем виброакустической маскировки с возможностью регулировки уровня помехи в каждом канале, используемом для зашумления того или иного элемента или конструкции. Оптимизация режима работы такой системы активного зашумления позволит снизить уровень побочных шумов и обеспечить большую комфортность ведения разговоров в защищаемом помещении.

Другим направлением повышения комфортности ведения разговоров является оптимизация спектра помехи, обеспечивающего выполнение требуемых норм по защите информации при минимальном интегральном уровне помехи.

В системах акустической и виброакустической маскировки используются шумовые, "речеподобные" и комбинированные помехи.

Наиболее часто из шумовых используются следующие виды помех:

1 - "белый" шум (шум с постоянной спектральной плотностью в речевом диапазоне частот);

2 - "розовый" шум (шум с тенденцией спада спектральной плотности 3 дБ на октаву в сторону высоких частот);

3 - шум с тенденцией спада спектральной плотности 6 дБ на октаву в сторону высоких частот;

4 - шумовая "речеподобная" помеха (шум с огибающей амплитудного спектра, подобной речевому сигналу).

В системах акустической и виброакустической маскировки, как правило, используются помехи типа "белого" и "розового" шумов.

В ряде систем виброакустической маскировки возможна регулировка уровня помехового сигнала. Например, в системах "Кабинет" и ANG осуществляется ручная плавная регулировка уровня помехового сигнала, а в системе "Заслон-2М" - автоматическая (в зависимости от уровня маскируемого речевого сигнала). В комплексе "Барон" возможна независимая регулировка уровня помехового сигнала в трех частотных диапазонах (центральные частоты: 250, 1000 и 4000 Гц). Система "Шорох-1" позволяет регулировать форму генерируемой помехи пяти полосным октавным эквалайзером.

"Речеподобные" помехи формируются (синтезируются) из речевых сигналов. При этом возможно формирование помехи как из скрываемого сигнала, так и из некоррелированных со скрываемым сигналом речевых фрагментов (отрезков).

Характерным представителем помех, формируемых из речевых фрагментов, некоррелированных со скрываемым сигналом, является помеха типа "речевой хор". Такая помеха формируются путем смешения фрагментов речи нескольких человек (дикторов).

Среди помех, формируемых из скрываемого сигнала, можно выделить два типа: "речеподобную" реверборационную и "речеподобную" инверсионную.

"Речеподобная" реверборационная помеха формируется из фрагментов скрываемого речевого сигнала путем многократного их наложения с различными уровнями.

"Речеподобная" инверсионная помеха формируется из скрываемого речевого сигнала путем сложной инверсии его спектра.

Комбинированные помехи формируются путем смешения различного вида помех, например помех типа "речевой хор" и "белый" шум, "речеподобных" реверборационной и инверсионной помех и т.п.

"Речеподобная" помеха типа "речевой хор" и комбинированная помеха типа "речевой хор" и "белый" шум реализованы в комплексе "Барон". Для этих целей в его состав кроме обычного генератора шума включены три радиоприемника, независимо настраиваемые на различные радиовещательные станции FM (УКВ-2) диапазона.

"Речеподобная" комбинированная (реверборационная и инверсионная) помеха используется в системе акустической маскировки "Эхо". Помеха формируется путем многократного наложения смещенных на различное время задержек разно уровневых сигналов, получаемых путем умножения и деления частотных составляющих скрываемого речевого сигнала.

Оценка эффективности шумовых помех осуществляется инструментально-расчетным методом, и обеспечивающим требуемую достоверность получаемых результатов оценки.

Оценка эффективности "речеподобных" помех, и особенно формируемых из скрываемого речевого сигнала, осуществляется методом артикуляционных испытаний (измерений).

Проведем оценку некоторых видов шумовых и "речеподобных" помех.

Методом математического моделирования с использованием формулы (1) получены зависимости словесной разборчивости W от интегрального отношения сигнал/шум q в полосе частот 180...5600 Гц при различном виде шумовых помех, которые представлены на рис. 7.1. В табл. 6 приведены значения отношений сигнал/шум в октавных полосах qi, при которых словесная разборчивость составляет W = 0,2; 0,3 и 0,4.

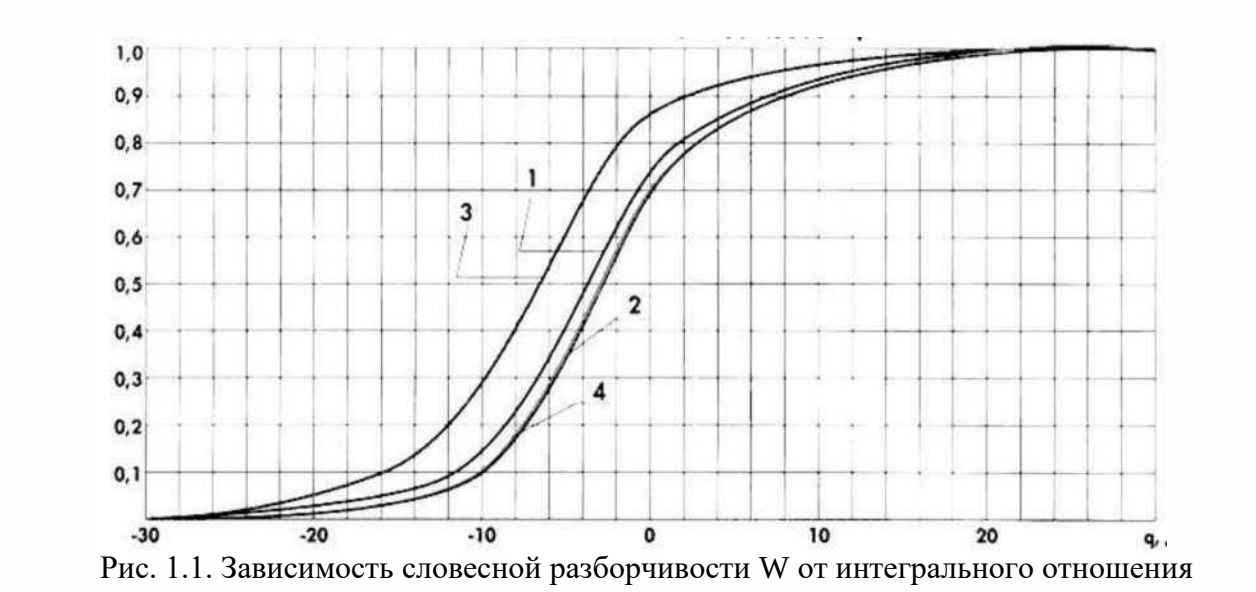


Рис. 1.1. Зависимость словесной разборчивости W от интегрального отношения сигнал/шум q в полосе частот 180.5600 Гц

1 - “белый” шум; 2 - “розовый” шум; 3 - шум со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот; 4 - шумовая “речеподобная” помеха

Анализ полученных результатов показал, что:

1. Наиболее эффективными являются помехи типа "розовый" шум и шумовая "речеподобная" помеха. При их использовании для скрытия смыслового содержания ведущегося разговора (W = 0,4) необходимо обеспечить превышение уровня помех над уровнем скрываемого сигнала в точке возможного размещения датчика средства акустической разведки на 4,9...5,0 дБ, а для скрытия тематики разговора (W = 0,2) - на 8,8.. .9,0 дБ.

2. Помеха типа "белого" шума по сравнению с помехами типа "розовый" шум и шумовая "речеподобная" обладает несколько худшими маскирующими свойствами, проигрывая по энергетике 0,8.. .1,2 дБ.

3. Значительно более низкими маскирующими свойствами обладает шумовая помеха со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот. По сравнению с помехами типа "розовый" шум и шумовая "речеподобная" она проигрывает по энергетике 4,1.. .4,2 дБ, а при равной мощности приводит к повышению разборчивости более чем в полтора раза.

1.4. Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса «СПРУТ-МИНИ»

Краткое описание используемого оборудования. 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 низкочастотных(НЧ) наводок на

токопроводящих элементах ограждающих конструкций, электроакустических преобразований в линиях технических средств передачи информации (ТСПИ) и за счет побочных электромагнитных излучений от технических средств в речевом диапазоне.

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 комплекса:

- диапазон измерений от 20 до 20000 Гц.;
- диапазон измеряемых уровней звукового давления - 10-105 дБ;
- диапазон измеряемых уровней виброускорений - 525 10 1 /мс;
- диапазон измеряемых уровней напряженности электрического поля - 5 10 10 /мкВ м;
- диапазон измеряемых уровней напряженности магнитного поля 4 0, 2 10 /мкА м;
- диапазон измеряемых уровней напряжений наведенного электрического сигнала - 235 10 10 мкВ.

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

В состав комплекса входят:

- управляющая ПЭВМ;
- программное обеспечение управления аппаратурой акустического контроля и обработки НЧ сигналов;
- многоканальный сигнальный концентратор «Спрут-МЗ»;
- блок формирования тестовых акустических сигналов «Спрут-ГЗ» с акустической системой;
- измерительный микрофон с принадлежностями;
- вибродатчик (акселерометр) с принадлежностями;
- антенны измерительные рамочная и дипольная.

Система виброакустического зашумления. Система виброакустического зашумления предназначена для создания виброакустических помех с целью защиты от прослушивания по акустическому и виброакустическому каналам.

Состав системы зашумления:

- блок генератора ANG-2200;
- вибрационные преобразователи TRN-2000;
- всенаправленные акустические излучатели OMS-2000.

ANG-2200 представляет собой 2 отдельных шумогенератора, создающих направленное зашумление. Вибрационный преобразователь TRN-2000 предназначен для защиты стен, окон, потолка, электропроводки, вентиляции. Всенаправленный акустический излучатель OMS-2000 предназначен для защиты пространства подвесных потолков, ниш, шкафов, вентиляционных коробов. Для каждого излучателя применяются различные крепежи, в зависимости от поверхности: стены, окна, системы трубопроводов и т.д. При помощи регуляторов высоких и низких частот возможно задание определенных параметров шума.

2. Порядок выполнения лабораторной работы

2.1. Оценка эффективности защиты речевой информации от утечки по акустическому каналу.

Оценка эффективности защиты речевой информации от утечки по акустическому каналу заключается в количественной оценке величины показателя эффективности защиты речевой информации и последующим ее сравнением с нормированными значениями.

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

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

Подготовка к работе:

- измерительный микрофон подключается ко входу третьего канала концентратора;
- подключается акустическая система к выходу «Акустическая система» генератора;
- подключается акустический излучатель OMS - 2000 к виброакустическому шумогенератору ANG -2200;
- подключается виброакустический шумогенератор к сети питания 220 В;
- выбирается контрольная точка;
- включается питание генератора;
- включается питание концентратора;
- если индикатор заряда аккумуляторных батарей (в правом верхнем углу жидкокристаллического индикатора (ЖКИ)) показывает, что батареи разряжены, то их следует зарядить с использованием штатного зарядного устройства.

Выполнение измерений.

Измеряется уровень тестового акустического сигнала, формируемого блоком внутри контролируемого помещения.

Устанавливается измерительное оборудование согласно рис.2.1.

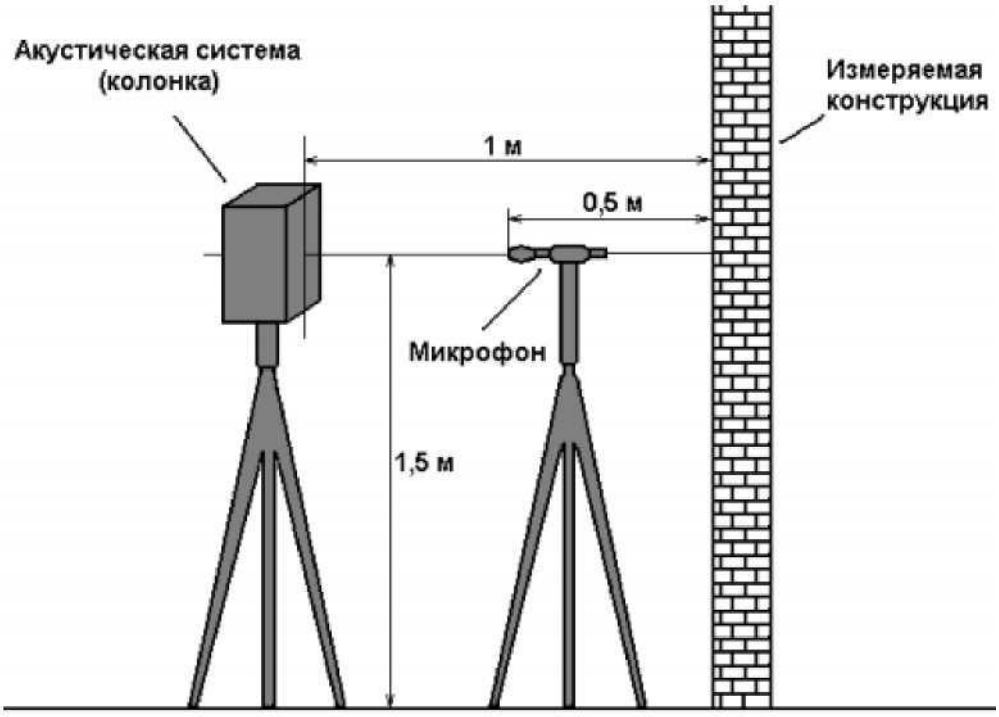


Рис. 2.1

Настраивается генератор:

- выбирается вид тестового сигнала «Шум», генератор переходит в режим выбора вида тестового сигнала при включении, выбор осуществляется с использованием курсорных кнопок пленочной клавиатуры ▲▼ и ◄► с последующим нажатием кнопки

Enter, после нажатия кнопки Enter прибор переходит в режим выбора вида шумового сигнала;

- выбирается вид шумового сигнала «Белый», выбор осуществляется с использованием кнопок ▲▼ и ◄► с последующим нажатием кнопки Enter, после нажатия кнопки Enter прибор переходит в меню корректировки спектра шумового сигнала;

- выбирается режим «Эквалайзер выкл», выбор осуществляется с использованием кнопок ◄► с последующим нажатием кнопки Enter, после нажатия кнопки Enter генератор переходит в режим регулировки уровня шумового сигнала;

- устанавливается уровень шумового сигнала «35», регулировка уровня шумового сигнала производится с использованием кнопок ◄►.

Включается шумовой сигнал.

Включение шумового сигнала на воспроизведение производится нажатием кнопки Enter пленочной клавиатуры генератора (выход из цикла воспроизведения шумового сигнала производится нажатием кнопки Out пленочной клавиатуры генератора).

Проводится единичное измерение.

Проведение единичного измерения производится из режима выбора коэффициента усиления. Для проведения единичного измерения необходимо нажать кнопку Start пленочной клавиатуры, при этом на нижнем поле экрана ЖКИ последовательно появятся надписи ВЫПОЛНЕНО и Enter-запись. Надпись ВЫПОЛНЕНО свидетельствует об окончании проведения единичного измерения.

Выключается шумовой сигнал.

Выключение шумового сигнала производится нажатием кнопки Out пленочной клавиатуры генератора.

Сохраняется результат измерения:

- осуществляется переход к банку памяти концентратора, который выполняется после проведения единичного измерения нажатием кнопки Enter, после чего на экране ЖКИ появится таблица результатов измерений, хранящихся в базе данных концентратора;

цифры первой колонки таблицы обозначают номер банка памяти концентратора, в котором хранятся результаты единичных измерений; буквенные сокращения во второй колонке обозначают тип датчика, с помощью которого проводилось измерение (ВИБ - вибродатчик, МИК - микрофон и ЛИН - линейный канал); буквенные сокращения третьей колонки идентифицируют вид измеряемого сигнала по трем категориям: тестовый сигнал (С), фоновый или помеховый сигнал (П) и суммарный сигнал (С+П); в четвертой колонке находится идентификатор проведенного измерения (имя

измерения), введенный пользователем;

- выбирается номер банка памяти для сохранения измерений, что осуществляется с использованием курсорных кнопок ▲▼ и нажатием кнопки Enter, после чего на экране ЖКИ появится запрос подтверждения записи;

- подтверждается запись в банк памяти, что осуществляется использованием курсорных кнопок ▲▼ и нажатием кнопки Enter, после чего на экране ЖКИ появится меню заполнения заголовка банка памяти концентратора;

- вводится имя проведенного измерения, что осуществляется с использованием курсорных кнопок ▲▼◄► и кнопки Enter;

- сохраняется имя проведенного измерения, что осуществляется после ввода имени нажатием кнопки Start, после чего на экране ЖКИ появится подтверждение сохранения имени измерения - СОХРАНЕНО, после этого появится экранная форма ввода вида измеряемого сигнала;

- выбирается вид измеряемого сигнала «Сигнал», что осуществляется с использованием курсорных кнопок ◄► и нажатием кнопки Start, после этого на экране ЖКИ появится подтверждение сохранения вида измеряемого сигнала - СОХРАНЕНО и автоматически загрузится список результатов измерений, хранящихся в базе данных концентратора с занесенными изменениями.

Измеряется уровень фонового шума в контрольной точке.

Устанавливается оборудование согласно рис.16.

Настраивается концентратор:

- осуществляется переход в режим «Проведение измерения», для чего нажимается кнопка Mode для перехода в меню выбора режима работы и в появившемся меню выбирается пункт «Проведение измерения»; выбор пункта меню прибора производится с использованием кнопок ▲▼ с последующим нажатием кнопки Enter;

- после нажатия кнопки Enter генератор переходит в режим регулировки уровня шумового сигнала;

- устанавливается уровень шумового сигнала «35», регулировка уровня шумового сигнала производится с использованием кнопок ◄►.

Сохраняется результат измерения:

- осуществляется переход к банку памяти концентратора, который выполняется после проведения единичного измерения нажатием кнопки Enter, после чего на экране ЖКИ появится таблица результатов измерений, хранящихся в базе данных концентратора;

цифры первой колонки таблицы обозначают номер банка памяти концентратора, в котором хранятся результаты единичных измерений;

- буквенные сокращения во второй колонке обозначаюттип датчика, с помощью которого проводилось измерение (ВИБ - вибродатчик, МИК - микрофон и ЛИН - линейный канал); буквенные сокращения третьей колонки идентифицируют вид измеряемого сигнала по трем категориям: тестовый сигнал (С), фоновый или помеховый сигнал (П) и суммарный сигнал (С+П); в четвертой колонке находится идентификатор проведенного измерения (имя измерения), введенный пользователем;

- выбирается номер банка памяти для сохранения измерений, что осуществляется с использованием курсорных кнопок ▲▼ и нажатием кнопки Enter, после чего на экране ЖКИ появится запрос подтверждения записи;

- подтверждается запись в банк памяти, что осуществляется использованием курсорных кнопок ▲▼ и нажатием кнопки Enter, после чего на экране ЖКИ появится меню заполнения заголовка банка памяти концентратора;

- вводится имя проведенного измерения, что осуществляется с использованием курсорных кнопок ▲▼◄► и кнопки Enter;

- сохраняется имя проведенного измерения, что осуществляется после ввода имени нажатием кнопки Start, после чего на экране ЖКИ появится подтверждение сохранения имени измерения - СОХРАНЕНО, после этого появится экранная форма ввода вида измеряемого сигнала;

- выбирается вид измеряемого сигнала «Сигнал», что осуществляется с использованием курсорных кнопок ◄► и нажатием кнопки Start, после этого на экране ЖКИ появится подтверждение сохранения вида измеряемого сигнала - СОХРАНЕНО и автоматически загрузится список результатов измерений, хранящихся в базе данных концентратора с занесенными изменениями.

Настраивается концентратор:

- осуществляется переход в режим «Проведение измерения», для чего нажимается кнопка Mode для перехода в меню выбора режима работы и в появившемся меню выбирается пункт «Проведение измерения»; выбор пункта меню прибора производится с использованием кнопок ▲▼ с последующим нажатием кнопки Enter;

- выбирается коэффициент усиления, равный 30 (выбор коэффициента усиления осуществляется с использованием курсорных кнопок ▲▼).

Измеряется уровень тестового акустического сигнала в контрольной точке.

Устанавливается оборудование согласно рис. 2.2.

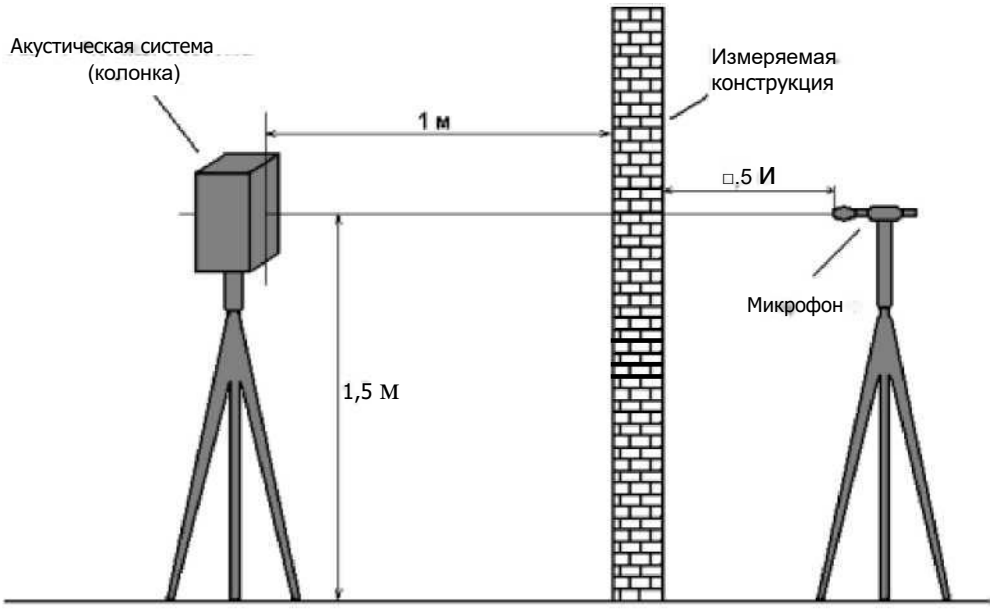


Рис. 2.2.

Устанавливается оборудование согласно рис.7.4. Включается и настраивается виброакустический шумогенератор.

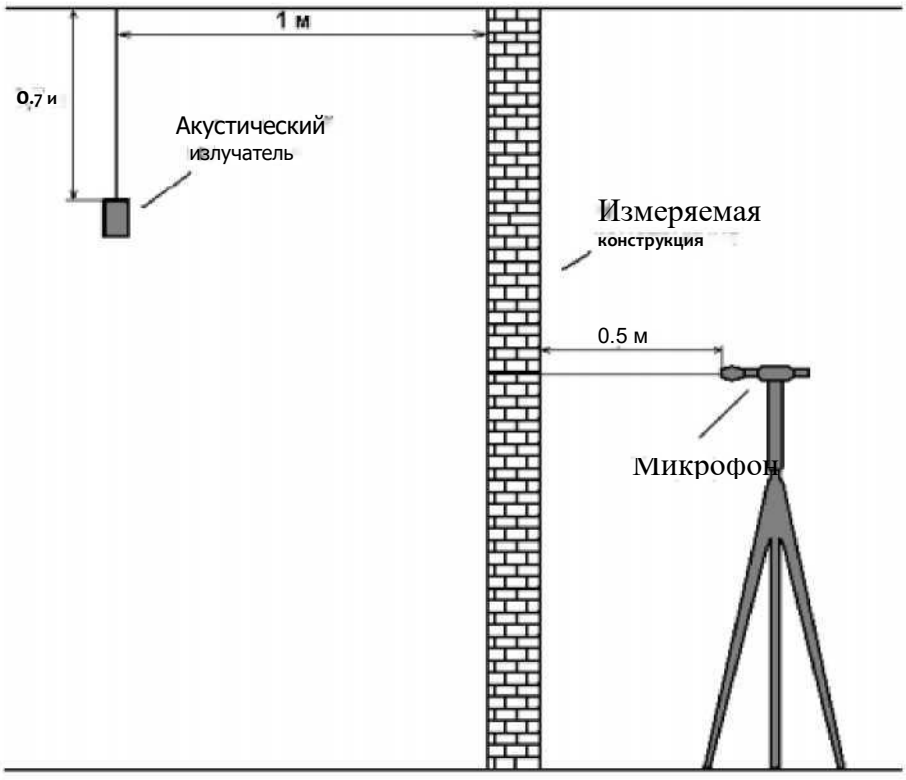


Рис. 2.3.

Выключается виброакустический шумогенератор нажатием кнопки Power ON.

4.1.2.4.6. Сохраняется результат измерения. Выбирается вид измеряемого сигнала «Помеха». Измеряется уровень тестового акустического сигнала и фонового шума в контрольной точке.

Настраивается концентратор. Включается и настраивается виброакустический шумогенератор. Включается шумовой сигнал нажатием кнопки Out пленочной клавиатуры генератора.

Проводится единичное измерение. Выключается шумовой сигнал нажатием кнопки Out пленочной клавиатуры генератора. Выключается виброакустический шумогенератор нажатием кнопки Power ON.

Сохраняется результат измерения, после сохранения имени проведенного измерения выбирается вид измеряемого сигнала «Сигнал + Помеха».

Измеряется уровень фонового шума, создаваемого системой виброакустического зашумления в контрольной точке. Измеряется уровень тестового акустического сигнала и фонового шума в контрольной точке.

Оформляется протокол № 1.

Выбирается вид контроля «Акустический», для чего нажимается кнопка выбора вида контроля, расположенная в верхней части главной экранной формы, и в появившемся меню выбирается вид контроля «Акустический контроль».

Выбирается категория НП, для чего нажимается кнопка выбора категории, расположенная в верхней части главной экранной формы, и в появившемся меню выбирается категория НП.

Открывается экранная форма «Работа с банками устройства»:

- осуществляется переход в экранную форму «Загрузка банка памяти концентратора из архива», для чего в главной экранной форме выбирается пункт главного меню «Файл», в списке файлов выбирается «Загрузка банков из архива»;
- осуществляется переход в экранную форму «Работа с банками устройства», для чего в правом окне экранной формы «Загрузка банка памяти концентратора из архива» выбирается имя файла, и дважды щелкается по нему левой кнопкой мыши;
- ставится галочка напротив сигнала + помехи;
- закрывается экранная форма «Работа с банками устройства».

Формируется и сохраняется протокол:

- нажимается кнопка «Расчет», после чего появится экранная форма «Просмотр результатов расчета»;
- нажимается кнопка «Протокол», после чего появится меню сохранения результатов измерения;
- выбирается пункт меню «Новый протокол», после чего появится протокол в формате «Документ Microsoft Word»;
- сохраняется «Документ Microsoft Word» под любым именем.

Содержание отчета:

- рисунки установок измерительного оборудования;
- результаты измерений, протоколы;

анализ полученных результатов и выводы.

Контрольные вопросы

1. Разборчивость речи при перехвате информации средствами разведки по прямому акустическому и виброакустическому каналам.
2. Ослабление акустических (речевых) сигналов.
3. Звукоизоляция строительных конструкций. Звукоизоляция оконных рам. Активные методы защиты.
4. Активные методы защиты.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1	1-2	1-3	1-3

Оценочные средства: ***отчет.***

Рачинский Сергей Андреевич

Лабораторная работа № 19-20

Тема: Исследование принципов формирования псевдослучайных последовательностей и методов их тестирования

Цель работы:

- приобрести навыки по созданию ГКП (генераторов ключевых потоков) для криптографических приложений;
- изучить методику тестирования генераторов случайных чисел (ГСЧ) и генераторов псевдослучайных чисел (ГПСЧ) на основе критериев американского стандарта FIPS 140-1.

Порядок выполнения работы

- выполнить ознакомительно – экспериментальную часть работы (п.1.1.);
- сформировать разными способами выборки случайных и псевдослучайных бит необходимого объема (п.1.2, 1.3);
- осуществить тестирование и проанализировать результаты (п.1.4);
- оформить отчет (п.1.5).

1.1 Ознакомительно – экспериментальная часть работы

1.1.1. **Изучить порядок функционирования ЛРР, используя демонстрационную программу (***ZIB_Lb2.exe***).**

Для этого необходимо выполнить следующее.

1) Выбрать пункт меню ***ЛРР → Демонстрация → Функционирование ЛРР …*** .

2) В открывшемся диалоговом окне «*Выбор образующего примитивного полинома*» выбрать один из приведенных (в списке) примитивных полиномов (рассмотреть для нескольких вариантов, в частности для тринома и для пентанома). (Используемые примитивные полиномы аналогичны первым триномам и пентаномам, приведенным в табл. А.1, А.2.)

3) Задать невырожденное начальное состояние регистра (либо <**Случайное**> либо <**Принудительное**> — задается самостоятельно).

4) Ознакомиться с порядком функционирования ЛРР в пошаговом режиме (кнопка <**Следующий такт**>): обратить внимание на закон формирования бита обратной связи и на формирование текущего выходного бита ЛРПМ (линейной рекуррентной последовательности максимального периода).

5) Ознакомиться со структурными свойствами сформированной ЛРПМ (см. краткое описание в приложении В), обратить внимание на ее длину (период $\boldsymbol{T}$) (сформировать несколько периодов ЛРПМ — кнопка <**До периода**>).

6) Сохранить полученную ЛРПМ — кнопка < **Сохранить полученную ЛРПМ** > и изучить ее свойства. Для этого выбрать пункт меню ***ЛРР → Демонстрация → Свойства ЛРПМ →*** **Прочитать ЛРПМ…** .

7) Добавить полученные результаты в промежуточный файл отчета (кнопка <**Добавить в отчет**>, по умолчанию имя файла отчета — report.txt). С примером содержимого автоматически формируемого файла отчета по данному режиму можно ознакомиться в приложении (см. прил. В).

В отчет **по лабораторной работе внести следующее:**

√ схемы выбранных ЛРР (для тринома и для пентанома);

√ трассировку нескольких (**(*m* + 3) ÷ (*m* + 8)**) тактов функционирования ЛРР с указанием для каждого следующей информации:

— состояние ЛРР;

— значение бита обратной связи ЛРР;

— значение выходного бита ЛРР;

√ значение периодов $\boldsymbol{T_i}$ сформированных ЛРПМ.

1.1.2. **Изучить особенности реализации и функционирования комбинированного генератора со сжатием, основанного на ЛРР, на примере упрощенной модели (один управляющий и один рабочий регистр) с примитивными образующими полиномами искусственно маленьких степеней** *m***.** Для этого необходимо, используя демонстрационную программу *ZIB_Lb2.exe***,** выполнить следующее.

2) Выбрать пункт меню ***ЛРР → Демонстрация → Комбинированный генератор → Генератор со сжатием …*** .

3) В появившемся диалоговом окне «*Демонстрация функционирования простейшего варианта генератора со сжатием*» задать структуру комбинированного генератора, выбрав из приведенных списков

образующие примитивные полиномы $\boldsymbol{f_1(x)}$, $\boldsymbol{f_2(x)}$ для задания управляющего (ЛРР$_1$) и рабочего (ЛРР$_2$) регистров соответственно. При этом начальные состояние обоих регистров задаются случайным (псевдослучайным) образом.

По умолчанию в комбинированном генераторе используется управляющий регистр ЛРР$_1$, заданный примитивным полиномом $\boldsymbol{f_1(x) = x^{12} + x^7 + x^4 + x^3 + 1}$, и рабочий регистр, заданный примитивным полиномом $\boldsymbol{f_2(x) = x^{13} + x^4 + x^3 + x + 1}$.

4) Ознакомиться с порядком функционирования заданного генератора со сжатием в пошаговом режиме (кнопка <**Следующий такт**>). Обратить внимание на закон формирования текущего выходного бита комбинированного генератора (на различие величин «*Текущий такт функционирования №*», «*Длина сформированной ПСП (бит)*», приведенных в соответствующих полях вывода).

5) Сформировав выходную ПСП объемом ***Len*** (бит), ***Len*** > $\boldsymbol{T_1}$, ***Len*** > $\boldsymbol{T_2}$ ($\boldsymbol{T_1}$ и $\boldsymbol{T_2}$ — периоды ЛРПМ исходных регистров ЛРР$_1$ и ЛРР$_2$ соответственно), обратить внимание на отличие периода формируемой выходной последовательности от периодов исходных регистров.

При этом для быстрого формирования выходной ПСП большой длины (без пошаговой демонстрации порядка функционирования) можно воспользоваться кнопкой <**Добавить *L* бит**>, которая позволяет добавить к текущей выходной последовательности ***L*** сформированных бит. (В открывшемся диалоговом окне выбрать длину ***L*** добавляемого к выходной последовательности отрезка ПСП.)

В отчет **по лабораторной работе внести следующее:**

√ выбранную схему генератора со сжатием;

√ образующие примитивные полиномы $\boldsymbol{f_1(x)}$, $\boldsymbol{f_2(x)}$;

√ периоды $\boldsymbol{T_1}$ и $\boldsymbol{T_2}$ исходных регистров (ЛРР$_1$, ЛРР$_2$);

√ трассировку нескольких (3 ÷ 6) тактов функционирования комбинированного генератора с указанием следующей информации:

— текущие состояния исходных ЛРР$_i$;

— текущие выходные биты комбинированного генератора;

√ вывод по соотношению величин периода ПСП, формируемой генератором со сжатием, и периодов $\boldsymbol{T_1}$, $\boldsymbol{T_2}$ исходных линейных рекуррентных регистров (ЛРР$_1$, ЛРР$_2$);

√ требования к выбору параметров комбинированного генератора такого типа с точки зрения сложности восстановления закона функционирования при использовании в реальных криптографических приложениях.

Таблица А.1 Примеры примитивных триномов степени m (m = 3, ..., 100)

№	Вид полинома $f(x)$	№	Вид полинома $f(x)$
1	$x^3 + x + 1$	21	$x^{20} + x^3 + 1$
2	$x^3 + x^2 + 1$	22	$x^{20} + x^5 + 1$
3	$x^4 + x^3 + 1$	23	$x^{21} + x^2 + 1$
4	$x^4 + x + 1$	24	$x^{22} + x + 1$
5	$x^5 + x^2 + 1$	25	$x^{23} + x^5 + 1$
6	$x^5 + x^3 + 1$	26	$x^{25} + x^3 + 1$
7	$x^6 + x + 1$	27	$x^{28} + x^3 + 1$
8	$x^6 + x^5 + 1$	28	$x^{29} + x^2 + 1$
9	$x^7 + x + 1$	29	$x^{31} + x^3 + 1$
10	$x^7 + x^3 + 1$	30	$x^{31} + x^{13} + 1$
11	$x^7 + x^4 + 1$	31	$x^{41} + x^3 + 1$
12	$x^7 + x^6 + 1$	32	$x^{41} + x^{20} + 1$
13	$x^9 + x^4 + 1$	33	$x^{52} + x^7 + 1$
14	$x^9 + x^5 + 1$	34	$x^{52} + x^{21} + 1$
15	$x^{10} + x^3 + 1$	35	$x^{63} + x + 1$
16	$x^{10} + x^7 + 1$	36	$x^{63} + x^5 + 1$
17	$x^{11} + x^2 + 1$	37	$x^{95} + x^{11} + 1$
18	$x^{15} + x + 1$	38	$x^{95} + x^{17} + 1$
19	$x^{17} + x^3 + 1$	39	$x^{100} + x^{15} + 1$
20	$x^{18} + x^7 + 1$	40	$x^{100} + x^{37} + 1$

Таблица А.2 Примеры примитивных пентаномов степени m (m = 6, ..., 30)

№	Вид полинома $f(x)$
1	$x^6 + x^5 + x^3 + x^2 + 1$
2	$x^8 + x^6 + x^5 + x + 1$
3	$x^{12} + x^7 + x^4 + x^3 + 1$
4	$x^{13} + x^4 + x^3 + x + 1$
5	$x^{14} + x^{12} + x^{11} + x + 1$
6	$x^{16} + x^5 + x^3 + x^2 + 1$
7	$x^{19} + x^6 + x^5 + x + 1$
8	$x^{24} + x^4 + x^3 + x + 1$
9	$x^{26} + x^8 + x^7 + x + 1$
10	$x^{27} + x^8 + x^7 + x + 1$

№	Вид полинома $f(x)$
11	
12	$x^{30} + x^{16} + x^{15} + x + 1$
13	
14	
15	
16	
17	
18	
19	
20	

1.2 Сформировать выборки псевдослучайных чисел длиной 20000 бит (2500 байт), используя ПО (программы CLinCongGener.exe и CLRRGener.exe), которое реализует ЛКГ и ЛРР. Значения параметров для образующих полиномов взять из соответствующих таблиц файла Приложение А по номеру машины.

1.3 Создать архивные файлы с помощью архиваторов zip и rar размером не менее 2500 байтов.

1.4 Осуществить тестирование всех полученных четырех выборок псевдослучайных чисел. Для тестирования используется программный комплекс FIPS 140-1. Запустить приложение TestFIPS1401.exe. Для осуществления тестирования необходимо:

- открыть файл, который содержит результаты работы генераторов, используя пункт меню “Файл”, “Открыть файл” или кнопку “Файл” на панели кнопок. Программа поддерживает возможность открытия нескольких файлов данных. Навигация по открытым файлам осуществляется с использованием кнопок “Назад” и “Вперед” на панели кнопок.
- для осуществления тестирования выбрать пункт меню “Файл“, “Тестирование” или нажать кнопку “Тестирование” на панели кнопок. После выполнения тестирования в поле окна выводятся результаты тестирования.

Программный комплекс позволяет:

– создавать отчеты в виде текстовых файлов, которые содержат результаты тестирования;
– создать демонстрационный отчет в виде файла в формате HTML;
– распечатывать результаты тестирования.

Используя результаты тестирования заполнить таблицу значениями статистических параметров :

Таблица 4

	Монобитный тест	Блочный тест	Тест серий						Тест длин серий
			1	2	3	4	5	6	
Rar									
Zip									
ЛКГ									
ЛРР									

Сделать выводы по каждому типу генераторов.

1.5 Содержание отчета.

Отчет должен содержать :

– цель исследований и программу работы;
– краткое описание генераторов;
– результаты, полученные на ознакомительном этапе работы (либо кнопка <**Добавить в отчет**>, по умолчанию имя файла отчета - report.txt.);
– итоговую таблицу с результатами;
– выводы по работе.

1.6 Контрольные вопросы.

1. Объясните процесс формирования псевдослучайных чисел с использованием ЛКГ.
2. Объясните процесс формирования псевдослучайной последовательности с использованием ЛРР.
3. Объясните процесс отбора псевдослучайных последовательностей по Fips-140.

Лабораторная работа № 21-22. «Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств»

Цель работы:

Целью данной лабораторной работы является изучение вопросов связанных с оценкой защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств.

1. Теоретическая часть

1.1. Краткие теоретические сведения

Практически в любом помещении находятся те или иные технические средства (ТС): это телефон, различные пожарные и охранные датчики, оргтехника, системы связи и т.д. И эти технические средства в нормальном режиме работы могут образовывать каналы утечки информации.

Достаточно хорошо известны способы несанкционированного получения информации об акустике помещения за счет подсоединения к линиям телефонных аппаратов (особенно аппаратов с электромеханическими звонками), линиям диспетчерской или громкоговорящей связи, вторичной часофикации, некоторым линиям охранной сигнализации и даже линиям электропитания. Подобные каналы утечки создаются за счет явления акустоэлектрических преобразований (АЭП) в элементах ТС.

Акустоэлектрический преобразователь - это устройство, преобразующее акустическую энергию (т.е. энергию упругих волн в воздушной среде) в электромагнитную энергию в схемах тех устройств, в которых находятся акустоэлектрические преобразователи. Наиболее распространенные акустоэлектрические преобразователи линейны, т.е. удовлетворяют требованиям неискаженной передачи сигнала, и обратимы, т.е. могут работать и как излучатель и как приемник (подчиняются принципу взаимности).

В основе явления АЭП лежат следующие физические эффекты:

• электродинамический эффект - возникновение ЭДС (тока) в обмотке, колеблющейся в магнитном поле;

• электромагнитный эффект - изменение магнитного потока через ферро магнитный сердечник при его механическом перемещении, вызванном акустическими колебаниями и, следовательно, изменение тока в его обмотке;

• электростатический эффект - изменение расстояния между обкладками конденсатора (например, воздушного) и следовательно изменение напряжения на нем;

• обратный эффект магнитострикции (эффект Веллари) - преобразование механической энергии, прикладываемой к сердечнику из магнитострикционного материала, в энергию магнитного поля, вызывающую ЭДС в обмотке. Такие конструкции используются в фильтрах, резонаторах и т.п.;

• пьезоэлектрический эффект - возникновение напряжения на поверхностях некоторых кристаллический веществ при их сжатии и растяжении;

• тензорезистивный эффект - изменение сопротивления полупроводниковых приборов при приложении к ним механических усилий.

Проявление акустопреобразовательных каналов утечки информации в большинстве случаев не связано с качеством исполнения того или иного технического средства, а является сопутствующим его деятельности. В ряде случаев они возникают за счет взаимности действия элемента, заложенного в конструкцию (динамики), в других случаях за счет некачественного исполнения элементов (рыхлая намотка индуктивностей, изменение расстояния между обкладками конденсатора и т.п.).

Таким образом, как следует из перечисления возможных механизмов преобразования, значительное количество элементов окружающих нас различных устройств,

может обладать акустопреобразовательным эффектом, и следовательно, может являться источником для создания канала утечки конфиденциальной акустической информации.

В данной работе применяется методика инструментально-расчетной оценки возможности утечки речевой конфиденциальной информации по каналам электроакустических преобразований, разработанная Гостехкомиссией России. Методика подразумевает оценку только прямых акустоэлектрических преобразований, т.е. тех, сигналы которых распространяются по проводам и частотный диапазон которых находится в частотном диапазоне речевого сигнала.

Метод оценки заключается в инструментально-расчетном определении совокупности октавных отношений напряжений, наводимых в функциональных (сигнальных) цепях ТС тестовым акустическим сигналом и шумом за счет их акустоэлектрических преобразований и последующим сравнением этих отношений с нормативными значениями.

1.2. Применяемое оборудование

Для измерений сигналов АЭП, как правило, имеющих крайне малые величины, в состав комплекса «Спрут-7» входят специальные дифференциальные усилители, выполненные в виде отдельных устройств. Каждый усилитель имеет внутренние аккумуляторы, фиксированные коэффициенты усиления 20, 40, 60 дБ. Кроме того, усилитель №2 имеет встроенный режекторный фильтр на частоту 50 Гц для уменьшения влияния наводок сети электропитания на результат измерений. Усилители позволяют измерять сигналы на симметричных и несимметричных проводных линиях. Если один из входов усилителя не используется, он закорачивается специальной заглушкой. В общем случае проводные линии необходимо исследовать в обоих режимах. Все измерения проводятся при отключенном питании исследуемого технического средства и при отсутствии напряжений на отходящих линиях. Исключение составляют телефоны и некоторые датчики пожарной сигнализации, при исследовании которых на них подается питание.

Внешний вид дифференциального усилителя приведен на рис. 1.1.

Рис. 1.1. Внешний вид дифференциального усилителя №1

На передней панели дифференциального усилителя расположен выключатель питания, а также прямой и инверсный входы усилителя. На задней панели усилителя расположен выходной разъем, через который усилитель подключается к измерительному модулю прилагаемым к комплексу кабелем, разъем для подключения зарядного устройства и переключатель коэффициента усиления.

Для питания телефонов, датчиков пожарной сигнализации и некоторых других технических средств в состав комплекса входит источник питания «SZPS-O!» (рис. 1.2).

Рис. 1.2. Внешний вид источника питания

Кроме питания ТС, источник питания «SZPS-01» предназначен для зарядки измерительных усилителей. Подключение ТС к источнику питания осуществляется через специальный переходник (рис. 1.3). К переходнику может непосредственно подключаться исследуемый телефонный аппарат, кроме того, на переходнике имеется разъем для непосредственного подключения дифференциального усилителя.

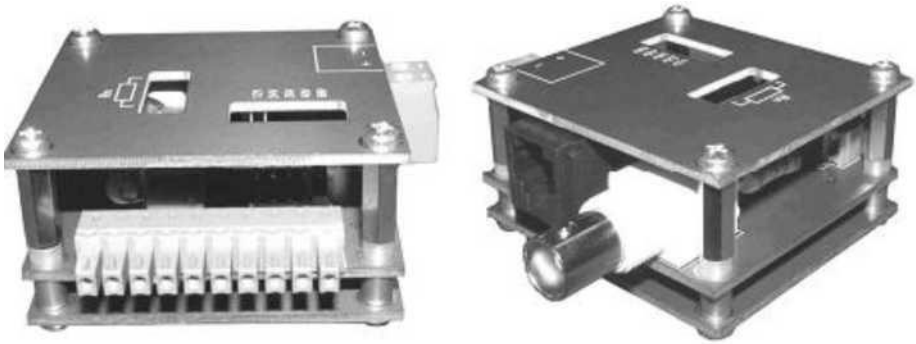


Рис. 1.3. Внешний вид переходника для подключения питания на технические средства

2. Порядок выполнения лабораторной работы

2.1.1. Изучить особенности заданного технического средства, предварительно оценить возможность возникновения АЭП.

2.1.2. Подготовить комплекс «Спрут-7» для проведения измерений АЭП.

2.1.3. Провести измерения сигналов АЭП.

2.1.4. Оформить протокол оценки защищенности помещения.

2.1.5. Ответить на контрольные вопросы.

2.2.1. Составьте план-схему размещения ТС в помещении, отметьте линии, выходящие за пределы помещения.

2.2.2. Подготовьте комплекс «Спрут-7» для проведения акустических измерений. Для этого:

- подключите модуль сопряжения к ПЭВМ;
- подключите измерительный микрофон к измерительному модулю.

Подключите антенну к измерительному модулю. Включите питание измерительного модуля;

- подключите источник тестового акустического сигнала к акустической системе. Включите питание источника тестового акустического сигнала (светодиод на передней панели модуля должен загореться зеленым светом). Включите питание акустической системы.
- запустите программное обеспечение для управления комплексом.

Через несколько секунд произойдет инициализация оборудования. Убедитесь, что:

- тип входного датчика - микрофон;
- кнопка «Полный спектр» отжата;
- чувствительность - низкая;
- фильтры 1/1 октавы;
- панель источника тестового сигнала - активна;
- уровень выходного сигнала источника тестового акустического сигнала - минимум;
- тип выхода - блокировка.

2.2.3. Измерение октавных уровней тестового акустического сигнала В качестве тестового акустического сигнала при измерении уровней АЭП необходимо использовать гармонические тональные сигналы с определенными уровнями. Поэтому необходимо «откалибровать» комплекс «Спрут-7».

Разместите микрофон на расстоянии 1м от АС. Используя программное обеспечение, на панели управления измерительным модулем включите режим графика №1 - текущий спектр.

На панели управления модулем акустического сигнала с помощью элемента «Синус» установите частоту выходного сигнала, в элементе управления «Выход» установите «Синус».

Нажмите кнопку «Пуск». С помощью регулятора уровня в панели источника тестового акустического сигнала начинайте увеличивать громкость воспроизводимого тонального сигнала. Измерения уровня производите курсором в окне анализатора спектра по центру соответствующей октавной полосы (не спутайте октавный уровень сигнала с интегральным).

Запишите значение регулятора уровня панели источника акустического сигнала в таблицу.

Повторите п. 2.3.2, п. 2.3.3, п. 2.3.4 для каждого значения необходимого частоты.

Завершите измерения уровней тестового акустического сигнала.

Выключите измерительный модуль, отключите и упакуйте измерительный микрофон.

2. 2.4. Измерение уровня октавного шума

Подключите ко входу измерительного модуля дифференциальный усилитель №1, 2. Входы усилителя при помощи прилагаемых осциллографических пробников подключите к исследуемой линии по симметричной (рис. 1.4) или несимметричной схеме (рис. 1.5).

Рис. 1.4. Симметричная схема подключения

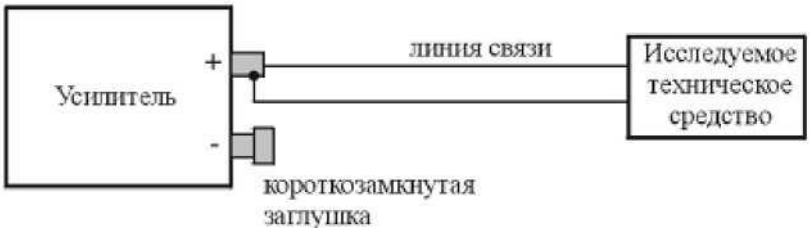


Рис. 1.5. Несимметричная схема подключения

Если исследованию подвергается ТС, требующее подачи питания (телефон, датчики пожарной сигнализации и т.п.), подключите питание ТС от источника питания «SZPS-01». К разъему переходника подключите один из входов дифференциального усилителя (в этом случае возможно только несимметричное подключение).

Включите дифференциальный усилитель.

Включите измерительный модуль.

Проведите настройку программного обеспечения (на панели датчиков):

- тип входного датчика - прямой вход;
- усилитель №1,2 (20 дБ, 40 дБ или 60 дБ) в зависимости от положения переключателя на задней панели усилителя.

На панели управления измерительным модулем включите режим графика №1 - текущий спектр. Нажмите кнопку «Пуск». В окне анализатора спектра должен отобразиться текущий спектральный состав напряжения шумов, присутствующих на входном разъеме дифференциального усилителя.

Перемещая курсор в окне анализатора спектра по центрам октавных полос, перепишите уровни сигналов в каждой октавной полосе в табл. 1, в графу $u_{ш.окт\ i}$, где i - номер октавной полосы (от 1 до 5).

2.2.5. Измерение уровней сигналов акустоэлектрических преобразований (АЭП)

Расположите АС на расстоянии 1 метр от исследуемого ТС.

В панели управления модулем акустического сигнала с помощью элемента «Синус» установите частоту выходного сигнала в соответствии с табл. 5.1, в элементе управления «Выход» установите «Синус». Уровень выходного сигнала для заданной выходной частоты установите на значение, соответствующее заданной частоте (табл. 5.1).

В окне анализатора спектра необходимо зафиксировать превышение уровня сигнала в i-й октавной полосе над уровнем шума $(U_{ш.окт\ г})$.

Если изменений нет или они слишком малы, попытайтесь увеличить коэффициент усиления дифференциального усилителя (20 дБ, 40 дБ), либо используйте другой усилитель (40 дБ, 60 дБ), а также изменить чувствительность измерительного модуля (элемент управления «Чувствительность»).

Запишите уровень измеренного сигнала в заданной полосе в таблицу 1.

Изменяя частоту и уровень выходного сигнала в соответствии с табл. 5.1, измерьте уровни сигналов в соответствующей октавной полосе и запишите их в табл. 1.

2.5.4. Измерения по п.2.5.1-2.5.3 необходимо провести для случаев симметричного и несимметричного подключения, а также для всех возможных режимов работы ТС, для каждого режима заполняя новую табл. 1. Например: при исследовании сигналов АЭП бытового вентилятора необходимо произвести измерения при всех возможных положениях переключателя скоростей и т.д.

2. 2.6. Завершение измерений

Выключите комплекс «СПРУТ-7». Для этого:

- завершите работу с программой;
- выключите АС выключателем питания;
- выключите модуль тестового акустического сигнала;
- выключите измерительный модуль;
- выключите дифференциальный усилитель;
- отключите модуль сопряжения;
- сложите все компоненты комплекса в сумку.

2. 2.7. Выполнение расчетов

Результаты измерений заносятся в табл. 5.2. Значения в графах «Уровень шума в линии связи, иш.окт i, мкВ» и «Уровень сигнала АЭП в линии связи U_c i , мкВ» рассчитываются по формуле 1. (дБ)

$$U(\text{мкв})=10^{20} \qquad (1)$$

Расчет отношения «сигнал/шум» в каждой октавной полосе производится по формуле 2.

$$\Delta i = \frac{U_{ci}}{U_{\text{ш окт } i}}. \qquad (2)$$

Таблица 1. Результаты измерений

Среднегеометрическая частота октавной полосы, Гц	Уровень шума в линии связи $U_{\text{ш.окт}\,i}$, дБ	Уровень шума в линии связи $U_{\text{ш.окт}\,i}$, мкВ	Уровень сигнала АЭП в линии связи U_{ci}, дБ	Уровень сигнала АЭП в линии связи U_{ci}, мкВ
250				
500				
1000				
2000				
4000				

Нормативное значение отношения «сигнал/шум» = 0,3, т.е. информация считается защищенной, если Ai < 0,3.

2.3. Содержание отчета

Отчетом по данной работе является протокол инструментально-расчетной оценки защищенности помещения от утечки речевой конфиденциальной информации (рекомендуемая форма протокола приведена в приложении), а также ответы на контрольные вопросы.

Контрольные вопросы

1. В чем заключается эффект акустоэлектрических преобразований?
2. Какие физические эффекты лежат в основе АЭП предложенного Вам в лабораторной работе технического средства?
3. Какие устройства с акустоэлектрическим эффектом могут входить в состав некоторых ВТСС?
4. В чем заключается эффект модуляционного акустоэлектрического преобразования?
5. В каком случае проводную линию следует рассматривать как несимметричную?
6. Назовите наиболее простой способ выявления факта модуляции сигнала модуляционного акустоэлектрического преобразователя.
7. По какому признаку делается вывод о наличии акустоэлектрических преобразований ВТСС?
8. Если акустоэлектрические преобразования обнаружены, то каким образом можно оценить их опасность?
9. Причины и последствия модуляции информационным речевым сигналом высокочастотных колебаний у генераторов технических средств.
10. Каким образом осуществляется перехват речевого сигнала в акустоэлектрическом канале?

ЛАБОРАТОРНАЯ РАБОТА №23-24
Тема « Поиск каналов утечки речевой информации»

Цель работы: изучить методы противодействия несанкционированному съему информации с помощью радиозакладок, получить навыки практического использования данных методов.

Задача: 1. Изучить теоретический материал методики работы с устройством СРМ-700.
2. Выполнить задания поиска закладного устройства.

Теоретический материал

СРМ-700 зонд-монитор - это универсальный прибор для обнаружения устройств скрытого съема информации. СРМ-700 - высококлассный прибор, разработанный для быстрого и незаметного обнаружения электронных устройств основных типов: передатчиков, работающих в диапазоне РЧ (от 50 кГц до 3 ГГц), ОНЧ (от 15 кГц до 1 МГц) и звуковых частот (от 100 Гц до 15 кГц).

В цикле лабораторных работ описываются различные способы применения СРМ-700, но он настолько совершенный и разносторонний прибор, что может использоваться и в методиках, оставшихся за пределами данной лабораторной работы. СРМ-700 дополняет полную методику обнаружения скрытых устройств на этапе физического поиска и визуального осмотра. Физический поиск, кроме того, может являться единственным способом обнаружения таких устройств, как: проводные микрофоны, волоконнооптические микрофоны, пассивные резонаторы, дистанционно управляемые "ждущие" устройства и другие устройства, которые невозможно обнаружить с помощью обычной аппаратуры.

СРМ-700 зонд/монитор объединяет в одном блоке пять наиболее необходимых при поиске функций (**В данной лабораторной работе рассмотрим одну из пяти функций поиска СРМ-700 - РЧ-зонд**):

Помните: физический поиск является базой для любой поисковой методики, он может дополняться и другими процедурами. Будьте предельно внимательны, смотрите тщательно.

1) РЧ-зонд обнаруживает скрытые микрофоны, импульсные передатчики и сигналы дистанционного управления, взрывные устройства.

2) ОНЧ-зонд обнаруживает "жучки", которые используют для передачи сигнала комнатную проводку.

3) сверхчувствительный усилитель на дополнительном входе позволяет прослушивать подозрительный телефон или проводку с целью обнаружения скрытых микрофонов или изменений в оборудовании.

4) функция "мониторинга опасности" т.е. слежения предназначена для защиты после поиска, она немедленно реагирует на присутствие нового устройства.

5) выход для непрерывной записи, сигнал с которого может подаваться на любой стандартный магнитофон, позволяет записать любые подозрительные звуки, пришедшие с зонда или дополнительного входа.

ДОПОЛНИТЕЛЬНЫЕ ЗОНДЫ И ТЕСТОВЫЕ ПЕРЕДАТЧИКИ

Возможности прибора могут быть значительно расширены при использовании дополнительных зондов. Для обучения обслуживающего персонала а также для тестирования прибора могут применятся тестовые передатчики.

MLP-700 Электомагнитный зонд. Для обнаружения каналов скрытых видеокамер и диктофонов.

IRP-700 Инфракрасный зонд. Предназначен для обнаружения, инфракрасных источников излучения

ALP-700 Акустический зонд. Предназначен для обнаружения каналов утечки акустической информации.

IRT-700 Тестовый инфракрасный передатчик

CCT-700 Тестовый передатчик с передачей по энергетической сети

ТТМ-700 Тестовый передатчик мощностью 0.7 мВт.

ОРГАНЫ УПРАВЛЕНИЯ

PHONES: для использования наушников и одновременного отключения внутреннего громкоговорителя .

GAIN: регулирует усиление звука (громкость) на громкоговорителе или выходе для наушников. Не влияет на уровень сигнала на выходе для записи.

FILTER: действует как полосовой фильтр в полосе речевых частот от 500 Гц до 2,5 кГц , убирает большую часть шума переменного тока на дополнительном входе и "видео" шума на входе для РЧ-зонда. Фильтр обрабатывает звуковые сигналы как для выхода на наушники, так и для выхода на запись.

MODE: Устанавливает прибор либо в режим поиска (search), либо в режим мониторинга(monitor). Режим поиска применяется при методичном обследовании помещения. Режим мониторинга применяется после поиска для постоянного отслеживания новых устройств.

Остальные функции группы MONITOR работают только в режиме мониторинга:

THRESHOLD: устанавливает мигающий сегмент на ЖК-дисплее в выбранную позицию. Когда значение входного сигнала превышает уровень, выставленный с помощью мигающего сегмента, прибор переключается в режим тревоги и подает сигнал на выход дистанционного управления.

ALERT: тревога, загорается красный светодиод.

SILENT: выключает звуковой сигнал при тревожном срабатывании, красный светодиод продолжает гореть.

INPUT LEVEL: отображает уровень входного сигнала с зонда или дополнительного входа; полулогарифмическая шкала с двумя диапазонами чувствительности.

PULSING SEGMENT: мигающий сегмент, устанавливает порог срабатывания сигнала тревоги в режиме мониторинга.

LOW BATT: индикатор напряжения питания, загорается при разрядке источника до 10%.

STATUS DISPLAY: показывает текущие положения органов управления и используемый вход.

PROBE: Входной разъем для приборных зондов, через него также идет питание для зондов. При присоединению зонда к прибору он автоматически переключается на этот вход. Используйте только зонды из комплекта СРМ

GAIN: Внутренняя чувствительность ЖК-дисплея и звуковых систем. В положении HIGH обеспечивается дополнительное усиление слабых входных сигналов.

A. AUXILIARY INPUT: дополнительный вход, сигнал с которого подается на высокочувствительный симметричный звуковой усилитель, используется при проверке проводки на наличие звуковых или управляющих сигналов.

B. METER: калибрует ЖК-дисплей при работе в режиме высокой (HIGH) чувствительности.

C. REMOTE: подает сигнал на вход дистанционного управления магнитофона для его включения/выключения

D. RECORD: подает звуковые сигналы, уловленные прибором, на микрофонный вход магнитофона

E. CHARGE: светодиод загорается при зарядке никель-кадмиевого аккумулятора.

F. ADAPTER: для подачи питания от сетевого адаптера и зарядки аккумулятора.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

РЧ-ЗОНД

Усиление: номинальное значение 20 дБ

Неравномерность АЧХ: 50 кГц - 2 ГГц _7+_ОЗдБ, 3 ГГц -10дБ

Чувствительность: -62 дБ относительно уровня 1 мВт (1 сегмент) -85 дБ относительно

1 мВт M.D. L.

Максимальный уровень входного сигнала' +15 дБ относительно 1 мВт, 50 В постоянного напряжения

Диапазон детектирования: 2 м при 1 мкВт 150 МГц 1/4_7 l_0 стандарт (усиление HIGH, значение дисплея 3 сегмента)

ДИСПЛЕЙ

18-сегментный ЖК-дисплей с двумя диапазонами чувствительности. Динамический диапазон 50 дБ (от 1 сегмента в режиме HIGH до MAX в режиме LOW)

СЕТЕВОЙ АДАПТЕР/ЗАРЯДНОЕ УСТРОЙСТВО

Вход 95-130 В или 200-275 В переменного напряжения 50-60 Гц

Выход. 12 В постоянного напряжения @ 500 мА

Время зарядки Ni-Cd аккумулятора: 8-10 часов

ВНИМАНИЕ!

Во избежание порчи прибора не превышайте следующих значений. РЧ-ЗОНД: *50 В постоянного напряжения +15 дБ относительно 1 мВт. Не касайтесь электрических цепей под напряжением!*

ПРИМЕЧАНИЕ: В РЧ-зонде содержится высокочувствительный усилитель, который может выйти из строя от электрического разряда через антенну. В условиях возможности появления статического электричества (сухие помещения, ковры) по возможности коснитесь исследуемого объекта сначала рукой, а только потом антенной

ПОИСК

Перед началом поиска следует учесть несколько пунктов.

Степень опасности CPM-700 рассчитан на широкий круг потребителей, начиная от представителей малого бизнеса, охраняющих свои частные секреты и до служб безопасности крупнейших корпораций и экспертов по технической защите информации Степень опасности может колебаться от низкой (спрятанные в мебель бытовые радиомикрофоны и телефонные "жучки") до очень высокой (специальная профессиональная современная техника) В последнем случае может понадобиться и другое поисковое оборудование и специальные методики

История здания. Установите не только сегодняшний уровень опасности, но и историю этого здания или помещения. Оцените возможность установки закладок во время строительства или оставшихся от предыдущих обитателей

Возможность доступа посторонних в охраняемое помещение. Проанализируйте, кто имеет возможность его посещать Поиск эффективен лишь до тех пор, пока помещение гарантировано от неконтролируемой установки новых устройств Установите порядок, кто, когда и куда имеет право быть допущенным

Потребности и возможности клиента. Независимо, работаете вы для себя, своей компании или для посторонних заказчиков, следует учитывать экономические соображения и степень желания и необходимости поддерживать меры безопасности

ВЫРАБОТКА ПЛАНА ДЕЙСТВИЙ

План может состоять в следующем:

Определение времени поиска. Искать следует тогда, когда "жучки" активны (обычно в рабочие часы)

Провоцирование к действию. Поскольку некоторые "жучки" могут быть дистанционно управляемы, то проведение фиктивных, но правдоподобных деловых переговоров побудит противоположную сторону активизировать свои устройства

Помощь. Люди, которым вы доверяете, могут оказать существенную помощь в процессе поиска

Неожиданность. Поиск следует проводить регулярно, но через случайные промежутки времени Более подробно это обсуждается в главе "Методы обнаружения"

Контролируемые утечки информации. Для выявления источника утечки информации можно организовать ее контролируемую утечку Только вы будете знать, что где и кому вы сообщили, а значит, станет ясен канал утечки Это может быть сделано посредством прослушивания, присутствия постороннего человека, не уничтоженного документа или другим способом

Поиск должен производиться скрытно, если вы ведете свою "контрразведывательную" игру Ваши разговоры с коллегами и заказчиком, приход, развертывание аппаратуры, ваш характерный шум и поиски "жучка" не должны дойти до противоположной стороны, если вы хотите снабжать его дезинформацией до того момента пока не обнаружили его устройство

МЕТОДЫ ОБНАРУЖЕНИЯ

ОКРУЖАЮЩЕЕ РАДИОИЗЛУЧЕНИЕ И ДИАПАЗОН ОБНАРУЖЕНИЯ

СРМ с РЧ-зондом обнаруживает передатчики звука и видео ("жучки"), работающие в полосе от 50 кГц до 3 ГГц. Двухдиапазонный дисплей покажет наличие радиоизлучения при приближении к его источнику, а принимаемый звуковой сигнал поможет отличить легальный местный источник от "жучка". Диапазон обнаружения СРМ-700 определяется в основном двумя главными факторами

1) мощностью передатчика-“жучка”, эффективностью и диаграммой направленности антенны,

2) окружающим радиоизлучением, например, местными коммерческими радио и ТВ станциями, двусторонней радиосвязью. В меньшей степени он зависит от рабочей частоты и длины антенны зонда

По мере приближения к источнику дисплей зафиксирует повышение интенсивности радиоизлучения. Это повышение может быть вызвано как обычным коммерческим ТВ или радиосигналом, так и нелегальным передатчиком Прослушивая его через наушники, вы отличите сигнал "жучка" и обычного радио или ТВ

После засекания сигнала нелегального передатчика следует локализовать зону с повышенным уровнем этого излучения, отслеживая его по дисплею. Для этой процедуры применяется "ходьба по кругу", которая позволяет очертить "горячую" зону

Не прерывайте режим скрытности после обнаружения жучка, так как их может быть несколько. Несколько жучков ставится для улучшения приема и для резервирования Если противоположная сторона знает о ваших подозрениях на прослушивание то они могут специально поставить одну или несколько легко обнаруживаемых закладок, чтобы убедить вас в успехе проведенного поиска и прекратить дальнейшие усилия

В СРМ-700 возможно реализовать обнаружение скрытых устройств по "звуковой обратной связи" В этом случае используется внутренний громкоговоритель прибора, который посылает звуковой сигнал в исследуемое помещение и активизирует закладки с микрофонами, которые одновременно транслируют этот же сигнал обратно, а он детектируется прибором и вызывает резкий звук в наушниках.

Помните: Противоположная сторона следит за своими устройствами и также будет слышать звук "обратной связи" Если жучок оснащен обратной связью, то он будет сразу выключен. Ваш поиск должен быть скрытным, постарайтесь не использовать опознаваемые звуки, так как это может только усугубить проблему.

Начинайте поиск только после тщательного знакомства с прибором и методиками обнаружения. Очень рекомендуется потренироваться в искусственных ситуациях перед реальным поиском.

ЗОНА КОНТРОЛЯ

Зоной контроля обычно является место, где ведутся наиболее важные переговоры (обычно это стол с телефоном). Большинство нелегальных устройств располагаются в радиусе 7 метров от этого места для лучшей слышимости и/или видимости.

ИСТОЧНИК "ИЗВЕСТНОГО ЗВУКА"

Во время поиска нелегальных устройств источник "известного звука" выполняет две очень важные функции

1) Он маскирует большинство шумов, производимых во время физического поиска.

2) Он работает как источник звука для "звуковой обратной связи" который не настораживает противоположную сторону и служит для выявления нелегальных устройств.

Источником "известного звука" может служить любой кассетный или CD-плейер, но лучшие результаты достигаются при использовании аппаратуры средних размеров, что объясняется размерами громкоговорителя.

Выберите наиболее уместную в данной ситуации запись, будь то музыка, бизнес-семинар или курс самообучения. Подберите соответствующую длительность, поскольку качественный поиск может занять много часов.

ПРИМЕЧАНИЕ: В качестве источника "известного звука не рекомендуется использовать радиоприемник, поскольку ту же станцию может поймать и СРМ-700, что может привести к ошибке и вы зафиксируете эту радиостанцию как нелегальный передатчик.

НЕЗАЩИЩЕННАЯ ЗОНА

Незащищенная зона используется для развертывания вашей аппаратуры. Это должно быть место, которое не вызывает интереса у противоположной стороны и не контролируемое ею, поэтому ваши действия останутся скрытыми.

ФИЗИЧЕСКИЙ ПОИСК

СРМ-700 должен применяться для обнаружения закладок обязательно в комбинации с тщательным физическим поиском/осмотром. Даже дорогой анализатор спектра не в состоянии обнаружить спрятанные устройства, если они находятся в пассивном состоянии или хорошо "зашиты" в обычную аппаратуру.

ПОВТОРНЫЙ ПОИСК

При повторных обследованиях можно сэкономить много времени, если скрытно пометить шурупы на стенных панелях, сетевых розетках, телефонных корпусах и/или других местах, куда могут быть установлены закладки Невидимое ультрафиолетовые маркеры и портативные источники УФ-излучения покажут нарушение целостности ранее обследованного объекта, если оно имело место. Соответствующие пометки в вашем журнале обследования помогут вам сориентироваться в будущей работе.

ПОДГОТОВКА К РАБОТЕ

КАЛИБРОВКА ПРИБОРА

СРМ-700 построен на современной элементной базе, дополненной температурной компенсацией параметров схемы, что обеспечивает стабильную и точную работу прибора. Из-за большого коэффициента усиления иногда требуется периодическая подстройка параметров, обусловленная старением элементов, изменений температуры и влажности среды

Если вы находитесь в условиях не очень интенсивного РЧ-излучения (10 сегментов и более при усилении high), точная калибровка не является необходимой.

НАУШНИКИ

ВНИМАНИЕ: Наушники для СРМ-700 обладают высоким качеством звучания и низкой слышимостью для окружающих. Не следует использовать уровень громкости в наушниках выше необходимого из-за возможности быть замеченными устройствами подслушивания (возможна обратная связь).

САМОДИАГНОСТИКА РЧ-ЗОНДА

Чувствительность РЧ-зонда может быть проверена в условиях низкого или среднего окружающего радиоизлучения Затем нужно максимально укоротить антенну и коснуться ее

концом шкалы дисплея. Исправный зонд будет выдавать "шум переключения" (хорошо слышимое гудение), неисправный очень тихое или вообще не выдавать, независимо от длины антенны.

ПОДГОТОВКА КОМНАТЫ

А. Закройте все окна и занавески для исключения визуального контакта

Б. Включите свет и все обычные офисные устройства, характерные для данного помещения.

В. Включите источник "известного звука" в центре зоны контроля для маскировки процедуры поиска.

Г. За пределами зоны контроля (в незащищенной комнате/зоне) как можно более бесшумно разверните вашу аппаратуру Д. Установите обычный уровень радиоизлучения окружающей Среды перед поиском в зоне контроля.

маркеры.

РЧ-ЗОНДИРОВАНИЕ

ВВЕДЕНИЕ

В этом разделе описано РЧ-зондирование и его применение для обследования помещений, телефонных линий и электропроводки, носимых микропередатчиков и следящих систем.

В РЧ-зонде содержится низкошумящий сверхширокополосный (50 кГц - 3 ГГц) усилитель, который способен работать со слабыми "уровня фона" сигналами, излучаемыми передатчиками. Уровень сигнала индицируется на дисплее в диапазонах низкой и высокой чувствительности и используется для "движения в направлении" источника радиоизлучения по самому высокому уровню.

ПРИМЕЧАНИЕ: В РЧ-зонде содержится высокочувствительный усилитель, который может выйти из строя от электрического разряда через антенну. В условиях возможности появления статического электричества (сухие помещения, ковры) по возможности коснитесь исследуемого объекта сначала рукой, а только потом антенной.

ВНИМАНИЕ! Не касайтесь зондом цепей с включенным питанием!

Модуляция: СРМ-700 чувствителен к амплитудной информации. Некоторые передатчики используют необычный тип модуляции, импульсный режим передачи данных или имеют очень узкую полосу частот. Они могут не обеспечить достаточного уровня звукового сигнала и не обеспечить хорошей слышимости источника "известного звука", а только индицировать его наличие на дисплее. Проверьте все "подозрительные" частоты.

Частоты: СРМ-700 и РЧ-зонд представляют собой широкополосный радиоприемник (50 кГц - 3 ГГц). Типичные "жучки" работают в диапазоне от 50 до 400 МГц. Более низкие частоты обуславливают применение больших антенн, что неприемлемо в реальной ситуации. Частоты выше 300 МГц плохо проходят через здания из-за отражения и поглощения.

Мощность: Нелегальные микропередатчики могут быть разделены на четыре группы: микромощные, маломощные, средней мощности и большой мощности. Зона вещания зависит не только от мощности, но и от формы и расположения приемной антенны, окружения, радиошума и параметров приемника. Передатчики большой мощности могут передавать сигнал на расстояние от 400 м и более с 100 мВт или выше. Передатчики средней мощности передают от 1 до 100 мВт на расстояние от 100 до 400м.

Маломощные жучки передают на менее чем 100 м, используя менее 1 мВт. Особую группу составляют микромощные передатчики, передающие 1 мкВт и менее . Они очень малы и с очень короткими антеннами. Монитор должен быть очень близко подноситься и быть очень чувствительным. Из-за непредсказуемости ситуации в применении нелегальных передатчиков обычно используется более чем минимально необходимая мощность для надежности.

ПОДКЛЮЧЕНИЕ РЧ-ЗОНДА

Следующие процедуры применяются при каждом подключении РЧ-зонда.

А.Подключите наушники, выставите минимальное усиление звука (против часовой стрелки).

Б. Поставьте переключатель режимов (Mode Switch) в позицию Search.

В.Присоедините РЧ-зонд к зондовому входу прибора (Probe) и разверните антенну на полную длину.

Г. Включите питание прибора и убедитесь в активации следующих текущих параметров.

Д. Установите уровень усиления. Если на дисплее индицируется высокий уровень шума (более 10 сегментов), то надо переключиться на низкий (low) уровень усиления и , если необходимо, укоротите антенну. Е. Настройте усиление звука до комфортабельного уровня.

ТИПИЧНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ ДЕЙСТВИЙ В КОМНАТЕ

А.Одев наушники и взяв РЧ-зонд за резиновую ручку, установите его вертикально перед собой, пока вы не вошли в обследуемое помещение.

Б. Входите в комнату, когда дисплей показывает среднее значение. Используйте усиление low, если дисплей показывает max (укоротите антенну, если дисплей показывает max при усилении low).

В.Выключите все приборы и свет в зоне контроля и близ нее и посмотрите , не изменились ли показания дисплея. Иногда обычная флюоресцентная лампа создает очень сильное радиоизлучение, в таком случае она должна быть выключена или удалена из комнаты. Если изменения в показаниях дисплея не могут быть вызваны такими явными причинами, то это означает реальное подозрение на "жучок".

Г. Повернитесь на 360 градусов вокруг, следя за показаниями дисплея, они будут меняться в зависимости от уровня радиоизлучения, существующего в комнате.

Д. Выделите направление с максимальным уровнем.

Е. Обследуйте все объекты, *в* которых могут быть спрятаны жучки. Если жучок рядом, то показания дисплея будут расти (в случае необходимости переключите усиление на low).

ПРИМЕЧАНИЕ: Иногда обнаруживается ложный источник сигнала где-то в воздухе, это значит, что реальный источник где-то рядом. Продолжайте поиск.

Ж. Необходимо идентифицировать выявленный источник радиоизлучения с целью отделить сигнал жучка от "нормального" сигнала. Слушая наушники, вы легко определите сигналы местных радио и ТВ-станций и двусторонней радиосвязи. Обнаружение сигнала "известного звука" означает обнаружение жучка.

ПОИСК В ПОМЕЩЕНИЯХ С СИЛЬНЫМ ФОНОМ

Следует заметить, что в некоторых помещениях, близких к мощным коммерческим телевизионным и радиопередатчикам придется использовать усиление low (показания дисплея более чем 10 сегментов). Обычно приходится следить за изменениями уровня сильных сигналов. Часто, если зонд расположен вблизи проводов или металлического объекта, дисплей будет показывать увеличение уровня сигнала, так же как и звук в наушниках станет громче. Это может означать не наличие жучка, а работу металлоконструкций как продолжение антенны. Проверьте это с помощью источника "известного звука".

В свободной продаже есть миниатюрные радиомикрофоны, работающие в коммерческом FM-диапазоне. Для соответствия требованиям Федеральной комиссии по связи он должен быть очень малой мощности, около двух микроватт. По этой причине он очень трудно обнаруживается с помощью

СРМ-700. К счастью, по этой же причине он малопригоден в качестве жучка из-за малого радиуса действия, менее 15 метров в большинстве случаев. В любом случае необходим тщательный физический поиск в дополнение к СРМ-700.

В местах с сильным радиофоном CPM-700 наиболее эффективен, если РЧ-зонд помещать напротив обследуемого объекта и следить, не превысит ли показание дисплея значение фона. Следует проверить все радиосигналы.

Задание на лабораторную работу

1. Установить CPM-700 на рабочем столе.
2. Подключите наушники, выставите минимальное усиление звука (против часовой стрелки).
3. Поставьте переключатель режимов (Mode Switch) в позицию Search.
4. Присоедините РЧ-зонд к зондовому входу прибора (Probe) и разверните антенну на полную длину.
5. Включите питание прибора и убедитесь в активации следующих текущих параметров.
6. Установите уровень усиления. Если на дисплее индицируется высокий уровень шума (более 10 сегментов), то надо переключиться на низкий (low) уровень усиления и, если необходимо, укоротите антенну.
7. Настройте усиление звука до комфортабельного уровня.
8. Одев наушники и взяв РЧ-зонд за резиновую ручку, установите его вертикально перед собой, пока вы не вошли в обследуемое помещение.
9. Входите в комнату, когда дисплей показывает среднее значение. Используйте усиление low, если дисплей показывает max (укоротите антенну, если дисплей показывает max при усилении low).
10. Повернитесь на 360 градусов вокруг, следя за показаниями дисплея, они будут меняться в зависимости от уровня радиоизлучения, существующего в комнате.
11. Выделите направление с максимальным уровнем.
12. Обследуйте все объекты, *в* которых могут быть спрятаны жучки. Если жучок рядом, то показания дисплея будут расти (в случае необходимости переключите усиление на low).

ПРИМЕЧАНИЕ: Иногда обнаруживается ложный источник сигнала где-то в воздухе, это значит, что реальный источник где-то рядом. Продолжайте поиск.

13. Необходимо идентифицировать выявленный источник излучения с целью отделить сигнал жучка от "нормального" сигнала. Слушая наушники, вы легко определите сигналы местных радио и ТВ-станций и двусторонней связи. Обнаружение сигнала "известного звука" означает обнаружение жучка.
14. Оформить отчет по приведенной далее форме.

ЛАБОРАТОРНАЯ РАБОТА № 25-26

Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.

1. Цель работы: ознакомление студентов с работой аппаратуры защиты информации, работающей в радиодиапазоне.

2. Краткие теоретические сведения (относятся к лабораторным работам № 2,3)

2.1. Радиоэлектронные каналы утечки информации.

В радиоэлектронном канале передачи носителем информации является электрический ток и электромагнитное поле с частотами колебаний от звукового диапазона до десятков ГГц.

Радиоэлектронный канал относится к наиболее информативным каналам утечки в силу следующих его особенностей:

- независимости функционирования от времени суток и года, существенно меньшая зависимость его параметров по сравнению с другими каналами от метеоусловий;
- высокой достоверности добываемой информации, особенно при перехвате ее в функциональных каналах связи;
- большого объема добываемой информации;
- оперативности получения информации вплоть до реального масштаба времени;
- скрытности перехвата сигналов и радиотеплового наблюдения.

В радиоэлектронных каналах утечки информации источниками сигналов могут быть:

- передающие устройства функциональных каналов связи;
- источники побочных электромагнитных излучений и наводок (ПЭМИН);
- объекты, отражающие электромагнитные волны в радиодиапазоне;
- объекты, излучающие собственные электромагнитные волны в радиодиапазоне.

Радиоэлектронные каналы в зависимости от вида источников сигналов делятся на каналы 1 и 2 вида. В каналах утечки первого вида производится перехват информации, передаваемой по функциональному каналу связи. С этой целью приемник сигнала канала утечки информации настраивается на параметры сигнала или подключается (контактно или дистанционно) к проводам соответствующего канала связи. Радиоэлектронный канал утечки второго вида имеет собственный передатчик сигналов, среду распространения и приемник сигналов. Передатчик сигналов этого канала утечки информации образуется случайно (без участия источника или получателя информации) или специально устанавливается в помещении злоумышленником. Такими передатчиками могут быть случайные источники опасных сигналов и закладные устройства.

2.2. Основные приборы и оборудование, применяемое для выявления радиоэлектронных каналов утечки информации.

Основными техническими средствами, предназначенными для выявления радиоэлектронных специальных технических средств (СТС) несанкционированного съема информации являются:

- индикаторы (детекторы) электромагнитного поля (ЭМП);
- скоростные приемники «ближней зоны»;
- универсальные поисковые приборы;
- автоматизированные многоканальные комплексы радиомониторинга.

Принцип действия индикаторов ЭМП основан на широкополосном детектировании

сигнала в контролируемом помещении. Основной способ обнаружения – амплитудный. Основные способы идентификации – индикатор уровня, частотомер, у наиболее совершенных моделей – идентификация известных цифровых сигналов.

Скоростные приемники «ближней зоны» являются сканирующими радиоприемниками. Поиск сигналов производится путем последовательного прохода всего диапазона с узкой полосой обзора в контролируемом помещении. Основной принцип идентификации опасных сигналов – анализ информации, заложенной в демодулированный сигнал. Способы индикации – световая, звуковая, индикатор уровня, частотомер, возможность прослушивания демодулированного сигнала.

Универсальные поисковые приборы объединяют в себе несколько функций:

- выявление радиоизлучающих СТС;
- выявление СТС, излучающих в инфракрасном диапазоне;
- выявление СТС, использующих проводные линии различного назначения;
- выявление источников ЭМП с преобладанием (наличием) магнитной составляющей поля;
- выявление наиболее уязвимых мест с точки зрения возникновения акустических и виброакустических каналов утечки информации.

Автоматизированные программно – аппаратные комплексы радиомониторинга применяются для организации непрерывного круглосуточного радиоконтроля охраняемых помещений для выявления закладных устройств. В их состав входят:

сканирующий радиоприемник;
контроллер;
компьютер с установленным на него специальным программным обеспечением;
антенный коммутатор;
внутренние и наружные антенны;
генератор прицельной помехи;
СВЧ конверторы.

2.3. Технические средства защиты информации от радиоизлучающих и проводных СТС.

Для защиты информации в данном случае используются генераторы линейного и пространственного зашумления. Первые подключаются к линиям различного назначения и подают в них электрические сигналы, перекрывающие опасные сигналы по спектру и мощности. Генераторы пространственного зашумления повышают уровень электромагнитных помех на входе приемника злоумышленника. Для эффективного подавления сигнала СТС уровень помехи в полосе спектра сигнала должен в несколько раз превышать уровень сигнала. Для подавления сигналов СТС применяются заградительные и прицельные помехи. Заградительные помехи имеют спектр, который перекрывает спектр сигналов подавляющего числа СТС, однако на долю узкополосного СТС приходится лишь незначительная часть энергии помехи, которой не хватает для эффективного искажения информационных параметров сигнала. Наращивание же мощности заградительной помехи ограничивается требованиями по экологической безопасности и электромагнитной совместимости излучений помех и сигналов радио вещания и связи в зашумляемом пространстве.

3. Краткое описание используемого оборудования

3.1. Детектор радиопередающих устройств PROTECT 1203.

Детектор поля PROTECT 1203 определяет наличие различных типов радиопередающих устройств и информирует об этом путем световой индикации и встроенного вибратора.

3.2. Универсальный поисковый прибор D 008.

Прибор D 008 предназначен для обнаружения и локализации СТС негласного получения информации, излучающих в радиодиапазоне, а также СТС, использующих для передачи информации линии сети переменного тока 220 В, абонентские телефонные линии, линии систем пожарной и охранной сигнализаций.

3.3. Портативный измеритель частоты и мощности MFP-8000.

3.3.1. Назначение.

Прибор MFP-8000 предназначен для измерения частоты и мощности радиосигналов.

3.3.2. Основные возможности прибора:

- измерение частоты сигнала в диапазоне от 100 кГц до 8 ГГц;

- измерение мощности сигнала в диапазоне от -60 до 30 дБм;

- Идентифицирование в сигнале признаков протокола обмена данными для сотовой и телефонной систем связи (GSM 900/1800/1900, DECT), в GSM определение режима работы SMS, Talk и значение частоты;

- автоматическое настраивание панорамных радиоприемников на измеренную частоту сигнала;

- использование встроенных памяти, часов и календаря для протоколирования и хранения результатов измерений;

- работа в составе автоматизированных систем мониторинга эфира;

- осуществление режима «акустозавязывания», используемого при проведении поисковых работ;

- поддержание сторожевого режима по критерию превышения мощности сигнала заданного порога.

3.4. Многофункциональный поисковый прибор ST031P (смотри описание в лабораторной работе №1).

3.5. Акустическая система.

3.6. Сотовый телефон стандарта GSM.

3.7. Имитаторы закладных устройств:

- радиомикрофон (РМК);

- телефонный радиоретранслятор параллельного подключения

(ТРП);

- видеокамера с радиоканалом передачи информации (ВКР).

3.8. Компьютер, видеопроектор, экран.

3.9. Генератор радиопомех ГШ-501 предназначен для работы в составе системы активной защиты информации, которая обеспечивает защиту информации от утечки по радиоканалам и каналам ПЭМИН путем создания широкополосной шумовой электромагнитной помехи в диапазоне частот от 0,01 до 1800 МГц.

3.10.Блокиратор сотовых телефонов, работающих в стандартах GSM 900/1800, DAMPS, CDMA, CDMA-2000-ЗАВЕСА-2.

4. Порядок выполнения работы

Лабораторная работа является демонстрационной и представляет собой рассказ и показ преподавателем принципов работы и применения современных технических средств обеспечения информационной безопасности, которые имеются в лаборатории в единичном количестве.

4.1. Работа с прибором PROTECT 1203.

4.1.1. Перед включением прибора отключено питание имитаторов закладных устройств. После включения прибора кнопкой POWER выдвигается его антенна и настраивается чувствительность ручкой SENS таким образом, чтобы светился или мигал только один сегмент на светоиндикаторе.

4.1.2. Включается питание скрытой ВКР. Вместе с прибором начинается обход лаборатории, наблюдая при этом показания прибора. Определяется место с наибольшим уровнем излучения, что подтверждается большим количеством светящихся на индикаторе сегментов и включением вибратора. Для более точного определения местонахождения ВКР по мере приближения к ней уменьшается чувствительность прибора. После определения точного местонахождения ВКР производится ее физический поиск, после чего показывается найденная ВКР и с помощью видеопроектора демонстрируется ее работа.

4.1.3. Включается питание генератора ГШ-501 и демонстрируется неспособность ВКР передавать видеоинформацию. Затем выключается питание генератора ГШ-501, прибора PROTECT

1203 и ВКР.

4.2. Работа с прибором D 008.

4.2.1. Начальное положение органов управления прибора:

- переключатель POWER в положении OFF;
- переключатель SOUND в положении SPEAK;
- кнопка MODE в положении HF;
- кнопка включения акустической обратной связи (АОС) в положении RF;
- ручки THRESHOLD и TUNING поворачиваются против часовой стрелки до упора.

4.2.2. Подключается телескопическая антенна к разъему ANT, переключатель POWER ставится в положение ON, вращением по часовой стрелке регулятора THRESHOLD устанавливается чувствительность таким образом, чтобы светился только первый сегмент шкалы индикатора.

4.2.3. Включается питание скрытого РМК. Вместе с прибором начинается обход лаборатории, наблюдая при этом показания прибора и слушая его звучания. Определяется место с наибольшим уровнем излучения, что подтверждается перемещением светящегося сегмента индикатора вверх по шкале уровня сигнала LEVEL и повышением тона звучания. Для более точного определения местонахождения РМК по мере приближения к нему уменьшается чувствительность прибора, а также включается режим АОС нажатием соответствующей кнопки в положение AUD.

После определения точного местонахождения РМК производится его физический поиск, после чего показывается найденный РМК и демонстрируется его способность передавать речевую информацию.

4.2.4. Включается питание генератора ГШ-501 и демонстрируется неспособность РМК передавать речевую информацию. Затем выключается питание генератора ГШ-501, прибора D 008 и РМК.

4.3. Работа с прибором MFP-8000.

4.3.1. Подключается телескопическая антенна к разъему INPUT прибора, он включается нажатием и удержанием кнопки включения/выключения на время порядка трех секунд. Кнопками MODE вверх-вниз, слева-направо выбирается режим Search и нажимается кнопка SET. Снова нажимается кнопка SET и в дальнейшем с помощью этой кнопки, кнопок MODE и кнопки Esc устанавливается ослабление аттенюатора 0 дБ, время измерения частоты сигнала 1 ms, единица измерения уровня сигнала watts.

4.3.2. Включается питание скрытого РМК. Вместе с прибором начинается обход лаборатории, наблюдая при этом показания прибора. Определяется место с наибольшим уровнем излучения, значение которого наблюдается на экране прибора в выбранных единицах измерения. При приближении антенны прибора к РМК на расстояние порядка нескольких сантиметров загорается зеленый светодиод LOCK и включается звуковая индикация о захвате частоты РМК, значение которой появляется на экране прибора, кроме того, там же индицируется мощность сигнала РМК.

После определения точного местоположения РМК производится его физический поиск, после чего показывается найденный РМК и демонстрируется его способность передавать речевую информацию, при этом на приборе нажимается и удерживается в нажатом состоянии кнопка AUD.

4.3.3. Включается питание генератора ГШ-501 и демонстрируется неспособность РМК передавать речевую информацию. Затем выключается питание генератора ГШ-501 и РМК.

4.3.4. Кнопками MODE, SET устанавливается режим работы прибора Pulse. Включается сотовый телефон, набирается номер и на экране прибора показывается значение частоты и режим работы телефона SMS или Talk, при этом загорается светодиод LOCK и включается звуковая сигнализация.

4.3.5. Включается питание блокиратора сотовых телефонов, что приводит к сбою в работе сотового телефона, о чем можно судить по информации, выводимой на его экран, а также по пропаданию световой и звуковой индикации прибора MFP-8000. Далее выключается питание блокиратора сотовых телефонов и прибора MFP-8000.

4.4. Работа с прибором ST031P.

4.4.1. Собирается схема лабораторной установки в соответствии с рис.8.

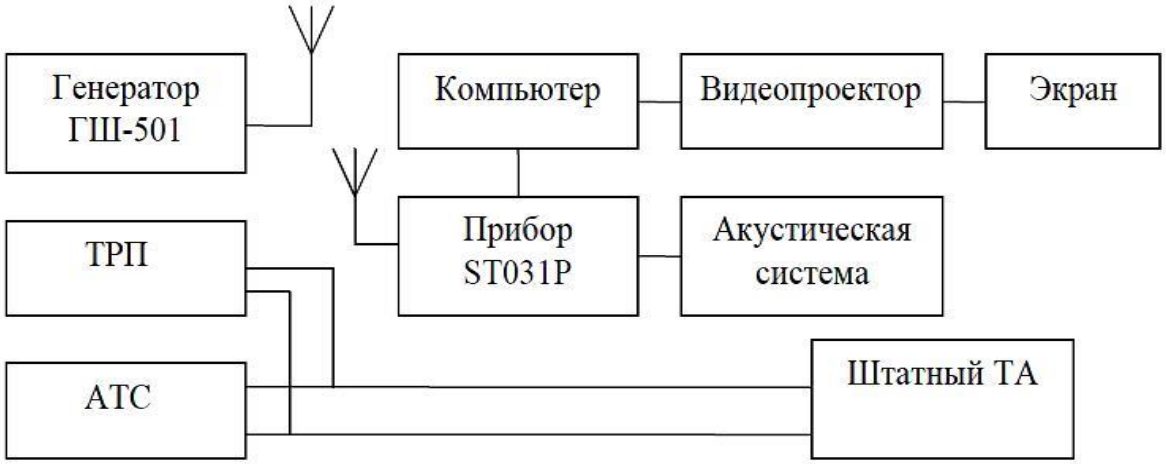


Рис.8

4.4.2. Подготавливается прибор ST031P к работе, для чего делается следующее:

- подключается высокочастотная антенна к разъему RF ANT;
- переключатель POWER ставится в положение ON;
- устанавливается порог детектора с помощью кнопок □□□, используя шкалу min - - - - I - - - - max, в такое положение, чтобы не было слышно щелчков в акустической системе.

4.4.3. Включается компьютер и видеопроектор, после чего на экране видеопроектора отображается информация с экрана прибора ST031P, что позволяет студентам отслеживать ее изменение при поиске ТРП.

4.4.4. Манипулируя антенной прибора, преподаватель добивается чередующихся тональных посылок (щелчков) в АС, частота которых увеличивается по мере приближения антенны к ТРП, при этом также увеличивается число окрашенных сегментов на шкале D индикатора прибора. После определения точного местонахождения ТРП производится его физический поиск, после чего показывается найденный ТРП и демонстрируется его способность передавать речевую информацию, при этом на приборе нажимаются кнопки MUTE и ENTER, то есть выбирается режим AUD.

4.4.5. Включается питание генератора ГШ-501 и демонстрируется неспособность ТРП передавать речевую информацию. Далее выключается питание генератора ГШ-501 и прибора ST031P.

5. Содержание отчета

5.1. Структурная схема лабораторной установки.

5.2. Результаты измерений, наблюдений и прослушиваний.

5.3. Анализ полученных результатов и выводы.

ЛАБОРАТОРНАЯ РАБОТА № 27-28

Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем охранной (пожарной) сигнализации

1. Цель работы: ознакомление студентов с работой аппаратуры защиты информации, работающей в проводных линиях различного назначения.

2. Краткое описание используемого оборудования

2.1. Многофункциональный поисковый прибор ST031P (смотри описание в лабораторной работе №1).

2.2. Универсальный поисковый прибор D 008 (смотри описание в лабораторной работе №2).

2.3. Акустическая система (АС).

2.4. Компьютер, видеопроектор, экран.

2.5. Генератор «белого шума» WNG 023.

Генератор «белого шума» WNG 023 предназначен для защиты переговоров от прослушивания с помощью СТС. Эффективен в замкнутом пространстве.

2.7. Генератор шума по сети электропитания и линиям заземления СОНАТА - РС1.

Генератор шума СОНАТА-РС1 предназначен для активной защиты от утечки информации в форме информативных электрических сигналов, возникающих в сети электропитания, системе заземления, инженерных коммуникациях.

2.8. Фильтр помехоподавляющий сетевой ФАЗА 1-10.

Фильтр предназначен для защиты однофазных цепей электропитания от высокочастотных помех в полосе частот от 30 кГц до 1000 МГц, обеспечивает защиту потребителей электроэнергии от кратковременных высоковольтных скачков напряжения, отключение потребителей от сети при превышении установленного максимального потребляемого тока, помехоустойчивость радиоэлектронных устройств и средств вычислительной техники.

2.9. Блок питания (БП).

2.10. Имитаторы закладных устройств:

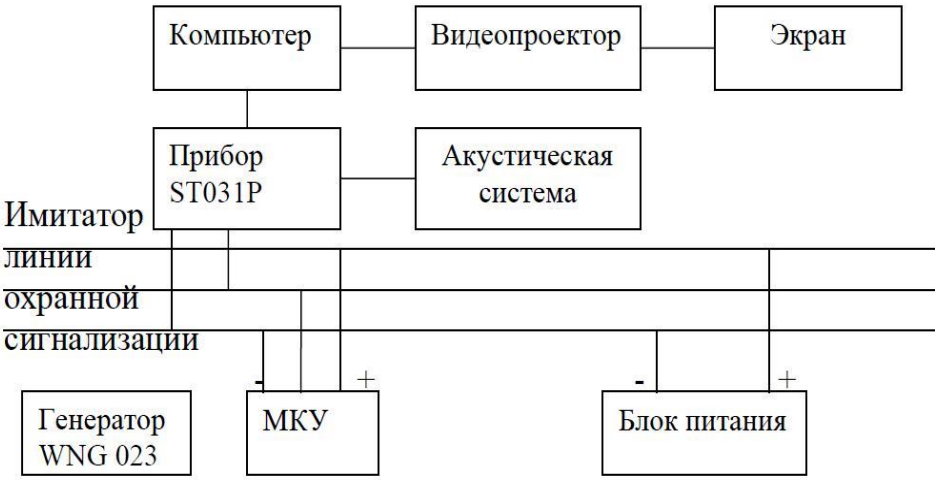
- микрофон с усилителем (МКУ);
- видеокамера с передачей сигнала по проводам (ВКП);
- закладное устройство, использующее для передачи информации силовые линии переменного тока (ЗУСЛ);
- имитатор линии охранной сигнализации.

3. Порядок выполнения работы

Лабораторная работа является демонстрационной.

3.1. Работа с прибором ST031P.

3.1.1. Собирается лабораторная установка в соответствии с рис.9.



3.1.2. Подготавливается прибор ST031P к работе, для чего делается следующее:

- к разъему PROBES подключается дифференциальный адаптер проводных линий;
- переключатель POWER ставится в положение ON.

3.1.3. Включаются компьютер и видеопроектор, после чего на экране видеопроектора студенты видят осциллограмму и параметры сигнала в линии охранной сигнализации.

3.1.4. Включается БП МКУ и питание генератора WNG 023, и студенты видят изменение сигнала и его параметров на экране видеопроектора, что позволяет сделать заключение о наличии в

линии закладного устройства (МКУ). Затем выключается генератор WNG 023.

После определения точного местонахождения МКУ производится его физический поиск, после чего показывается найденный МКУ и демонстрируется с использованием АС его способность передавать речевую информацию. Далее снова включается генератор WNG 023 и демонстрируется неспособность МКУ передавать речевую информацию. Затем выключаются БП МКУ, генератор WNG 023 и прибор ST031P.

3.1.5. Собирается лабораторная установка в соответствии с рис.10.

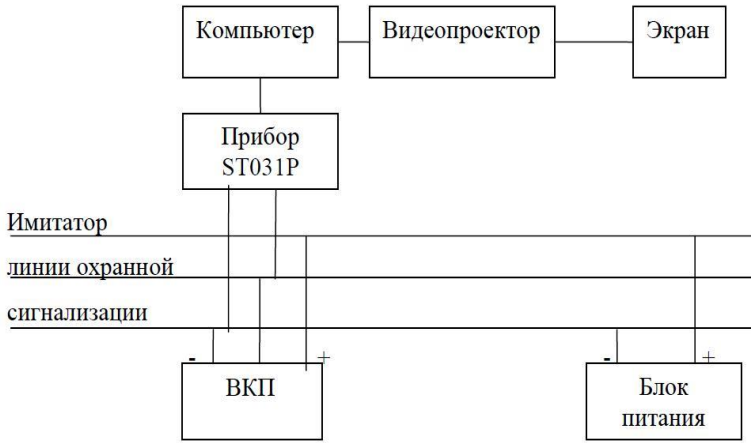


Рис.10

3.1.6. Подготавливается прибор ST031P к работе, для чего делается следующее:

- к разъему OSC2 подключается высокочастотный кабель;

- переключатель POWER ставится в положение ON;
- нажимается кнопка OSC два раза в течение двух секунд;
- кнопкой устанавливается максимальный предел горизонтальной развертки 36,5 мсек. (информация индицируется в правом нижнем углу экрана прибора);
- кнопкой ▼ устанавливается максимальный предел вертикальной развертки 279 мВ (информация индицируется в левом верхнем углу экрана прибора);
- нажимается кнопка SET, после чего появляется меню, и кнопкой 3 выбирается режим PEAK DETECT measure, кнопкой 4 – Trigger ON in STOP, кнопкой 5 – Trigger run < LEVEL, нажимается кнопка ENTER.
- Включается БП ВКП, нажимается кнопка RUN/STOP, и на экране прибора наблюдается изображение сигнала, похожее на изображение телевизионного сигнала. Для проверки выключается свет в лаборатории, снова нажимается кнопка RUN/STOP и наблюдается изменение изображения сигнала, что позволяет сделать заключение о наличии в линии закладного устройства (ВКП).

После определения точного местонахождения ВКП производится ее физический поиск, после чего показывается найденная ВКП и демонстрируется с использованием видеопроектора ее способность передавать видеоинформацию. Далее выключаются БП ВКП, прибор ST031P.

Собирается схема лабораторной установки в соответствии с рис.11.

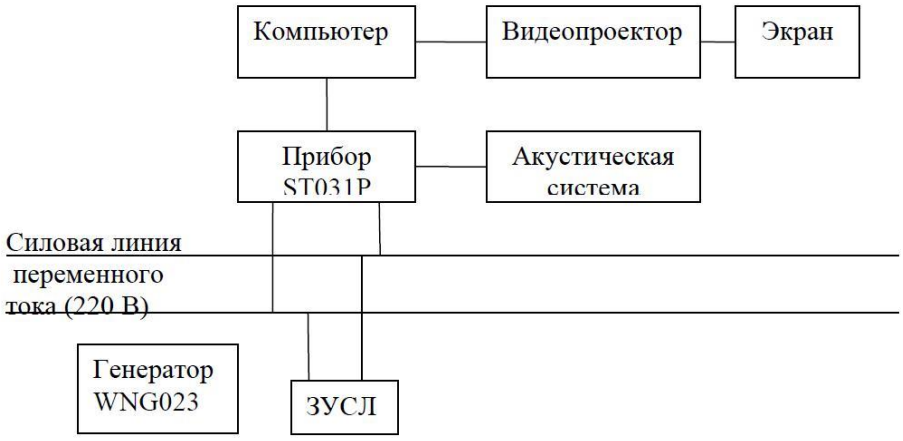


Рис.11

3.1.9.Подготавливается прибор ST031P к работе, для чего делается следующее:

- адаптер сканирующего анализатора проводных линий подключается к разъему PROBES, на нем загораются два светодиода, его переключатель ставится в крайнее правое положение;
- переключатель POWER ставится в положение ON;
- нажимается кнопка 7 для уменьшения уровня громкости встроенного динамика до нуля.

3.1.10. Устанавливаются нижняя и верхняя частоты сканирования: нажимаются кнопки SET и 4, вводятся значения частот 00.300 и 00.500 МГц с использованием кнопки

ENTER, при этом на экране видеопроектора наблюдается амплитудный спектр сигнала в силовой линии и бегающий вдоль оси частот курсор; нажимается кнопка ENTER для установки частотного демодулирования (FM), что подтверждается в верхней строке индикатора; кнопками ▲▼ устанавливается порог остановки сканирования по максимальной составляющей спектра, после настройки анализатора на эту составляющую включается питание генератора WNG 023, и студенты прослушивают сигнал этого генератора, что позволяет сделать заключение о наличии в линии закладного устройства (ЗУСЛ). Затем выключается генератор WNG 023.

После определения точного местонахождения ЗУСЛ производится его физический поиск, после чего показывается найденный ЗУСЛ и демонстрируется с использованием АС его способность передавать речевую информацию.

3.1.11. Собирается схема лабораторной установки в соответствии с рис. 12.

3.1.12. Переключатель фильтра Ф1-10 ставится в положение RESET, после чего загораются светодиоды на адаптере сканирующего анализатора проводных линий; нажимается кнопка RUN/STOP, начинается сканирование силовой линии, и студенты видят на экране видеопроектора, что после фильтра Ф1-10 отсутствует сигнал ЗУСЛ.

3.1.13. Выключается питание прибора ST031P, компьютера и видеопроектора.

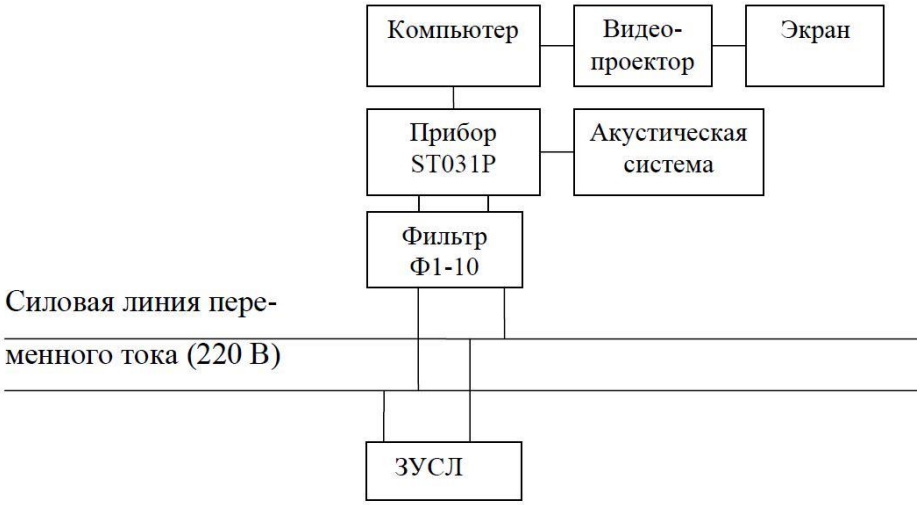


Рис. 12

3.2. Работа с прибором D 008.

3.2.1. Собирается схема лабораторной установки в соответствии с рис. 13.

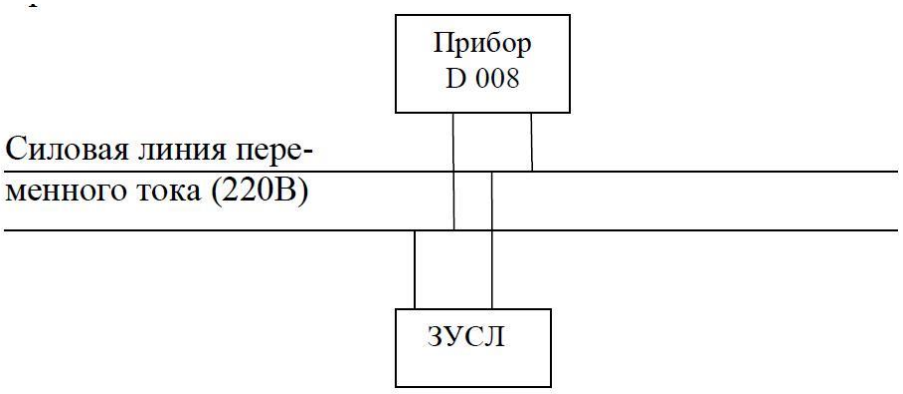


Рис. 13

3.2.2. Подготавливается к работе прибор D 008, для чего делается следующее:

- переключатель SOUND ставится в положении SPEAK;
- кнопка MODE нажимается в положение LF;
- кнопка включения акустической обратной связи (АОС) нажимается в положение AUD;
- ручки THRESHOLD и TUNING поворачиваются против часовой стрелки до упора;
- к разъему LF INPUT подключается адаптер проводных линий;
- переключатель POWER ставится в положении ON.

3.2.3. Вращением ручки TUNING по часовой стрелке производится перестройка прибора D 008 по частоте до появления в динамике прибора громкого характерного звука, обусловленного возникновением акустической обратной связи, при этом пропадание этого звука после нажатия кнопки АОС в положение RF говорит о наличии в линии ЗУСЛ.

После определения точного местонахождения ЗУСЛ производится его физический поиск, после чего показывается найденный ЗУСЛ и демонстрируется его способность передавать речевую информацию.

3.2.4. Собирается схема лабораторной установки в соответствии с рис. 14.

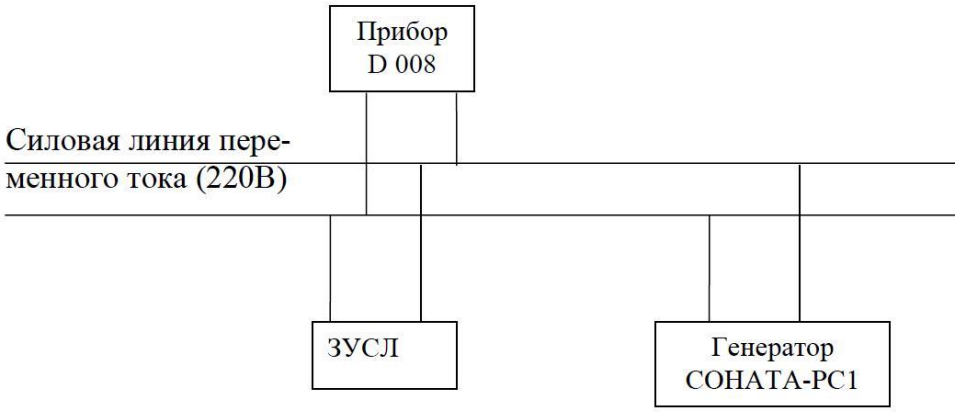


Рис. 14

3.2.5. Включается питание генератора СОНАТА-РС1 и демонстрируется неспособность ЗУСЛ передавать речевую информацию. Затем выключается питание прибора D 008 и генератора СОНАТА-РС1.

4. Содержание отчета

4.1. Структурные схемы лабораторных установок.

4.2. Результаты измерений, наблюдений и прослушиваний.

4.3. Анализ полученных результатов и выводы.

Лабораторная работа №29-30

Тема: Исследование принципов построения симметричных криптосистем и их использования для защиты данных

Цель работы.

- изучить особенности современных блочных симметричных шифров;
- изучить режимы применения симметричных шифров для обеспечения конфиденциальности данных;
- получить практические навыки по построению систем обеспечения конфиденциальности данных.

Теоретическая часть

- повторить требования к симметричным блочным шифрам;
- повторить алгоритмы шифрования, дешифрования, которые реализованы в стандартах DES и ГОСТ 28147-89;
- изучить особенности современных блочных симметричных шифров;
- изучить особенности, достоинства и недостатки режимов применения блочных симметричных шифров.

1. Алгоритм шифрования ГОСТ 28147-89

Алгоритм ГОСТ 28147-89 - это алгоритм криптографического преобразования данных, предназначенный для аппаратной или программной реализации, который удовлетворяет криптографическим требованиям и не налагает ограничения на степень секретности защищаемой информации.

В алгоритме ГОСТ 28147-89 предусмотрены 4 режима шифрования.

1. Режим простой замены - может использоваться в основном для шифрования ключевых данных.
2. Режим гаммирования - применяется для поточного шифрования без аутентификации.
3. Режим гаммирования с обратной связью используется для поточного шифрования с аутентификацией.
4. Режим выработки имитовставки - используется для аутентификации информации и может применяться вместе с каждым из режимов шифрования.

Математическое описание алгоритмов шифрования и дешифрования.

В алгоритме ГОСТ 28147-89 используются следующие элементарные криптографические преобразования:

- подстановка 4-разрядных векторов;
- перестановка 32-разрядных векторов;
- сложение по модулю 2;
- сложение по модулю 2^{32};
- сложение по модулю 2^{32}-1.

В алгоритме используется сеансовый ключ X и долгосрочный ключ K. Ключ X имеет длину 256 бит и может быть представлен в виде вектора с 8 32-разрядных слов X(7) X(6)...X(0). Ключ K состоит из 8 таблиц подстановок K(1), K(2) ., K(8), каждая из которых задает 4-битовую подстановку.

При описании алгоритма будем использовать следующие обозначения.

Если *L* и *R* - последовательности бит, то их конкатенацию (сцепление) будем помечать через *LR*.

Символом □□ обозначается побитное сложение по модулю 2. Символом [+]обозначается сложение по модулем 2^{32}:

$$A[+]B = \begin{cases} A+B; \text{если } A+B < 2^{32} \\ A+B-2^{32}; \text{если } A+B \geq 2^{32} \end{cases} \quad (1)$$

Символом {+} обозначается сложение по модулю 2^{32}-1:

$$A\{+\}B = \begin{cases} A+B; \text{если } A+B < 2^{32} \\ A+B-(2^{32}-1); \text{если } A+B \geq 2^{32} \end{cases} \quad (2)$$

Работа алгоритма ГОСТ 28147-89 в режиме простой замены.

Открытые данные T, которые подлежат шифровке, разбиваются на блоки T(k) длиной 64 бита. Последовательность битов T(k) разделяется на 2 последовательности A(0) и B(0) длиной 32 бита. Потом выполняется итеративный процесс шифровки, который описывается формулами:

$$A(i) = f_ш(A(i-1)\ [+]\ X(j)) \square\square B(i-1);$$
$$B(i) = A(i-1); \quad (3)$$

для i = $\overline{1,24}$; j = (i-1) mod 8;

$$A(i) = f_ш(A(i-1)\ [+]\ X(j)) \square\square B(i-1);$$
$$B(i) = A(i-1); \quad (4)$$

для i = $\overline{25,31}$; j = 32-i;

$$A(32) = A(31);$$
$$B(32) = f_ш(A(31)\ [+]\ X(0)) \square\square B(31); \quad (5)$$

для i= 32; где i - номер итерации; fш - функция шифровки.

64 - разрядный блок зашифрованных данных Ш(k) представляется в виде:

$$Ш(k) = A(32)\ B(32). \quad (6)$$

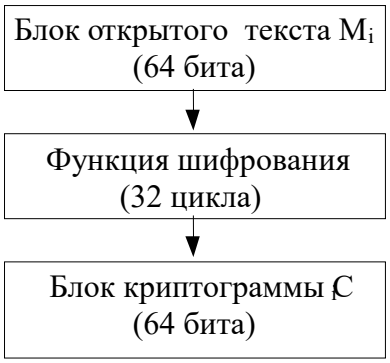


Рисунок 1. Схема алгоритма ГОСТ в режиме простой замены

Функция шифровки fш включает две операции (рис. 9). Первая операция - подстановка. Блок подстановки К состоит из 8 узлов замены К(1),...,К(8) с памятью 64 бит каждый. 32-разрядный вектор, что поступает на блок подстановки, разбивается на 8 4-разрядных векторов, каждый из которых превратится в другой 4-разрядный вектор соответствующим узлом замены, что представляет собой таблицу из 16 целых чисел в диапазоне 0..15. Ключ подстановки является долгосрочным.

Вторая операция - циклический сдвиг влево 32-разрядного вектора, полученного в результате подстановки К.

Функция шифрования

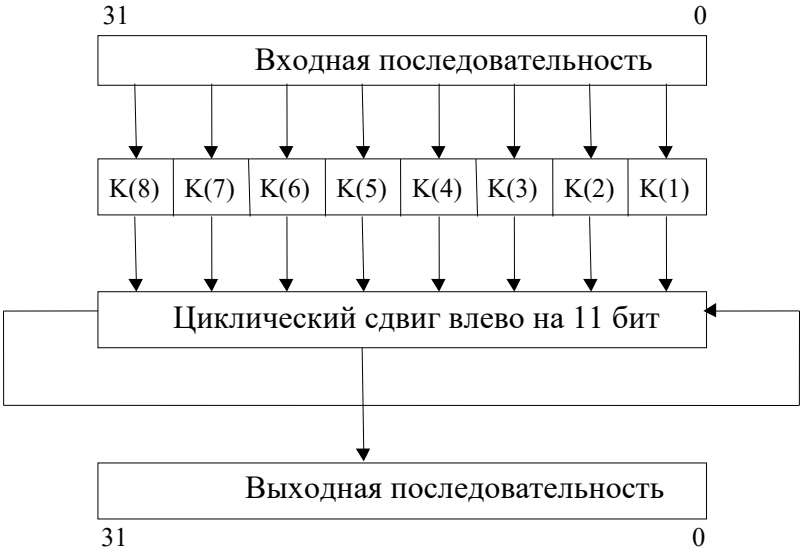


Рисунок 2. Ход шифрования

Процесс дешифровки в режиме простой замены осуществляется по формулам:

$$A(0)\ B(0) = Ш\ (k) \quad (7)$$

$$A(i) = f_{ш}(A(i-1)\ [+]\ X(j))\ \square\square B(i-1);$$
$$B(i) = A(i-1); \quad (8)$$

для $i = \overline{1,8}$; $j = i-1$;

$$A(i) = f_{ш}(A(i-1)\ [+]\ X(j))\ \square\square B(i-1);$$
$$B(i) = A(i-1); \quad (9)$$

для $i = \overline{9,31}$; $j = (32-i) \bmod 8$;

$$A(32) = A(31);$$
$$B(32) = f_{ш}(A(31)\ [+]\ X(0))\ \square\square B(31); \quad (10)$$

для i = 32;
где i - номер итерации.

$$T(k) = A(32)\ B(32). \quad (11)$$

Работа алгоритма ГОСТ 28147-89 в режиме гаммирования

Открытые данные T, которые подлежат шифровке, разбиваются на блоки T(j) длиной 64 битов.

Уравнение шифровки данных может быть представлено в следующем виде:

$$Г(i) = A(Y(i-1)\ [+]C2,\ Z(i-1)\ \{+\}C1\ ) \quad (12)$$

$$Ш(i) = Г(i)\ \square\square T(i) \quad (13)$$

где Ш(i) - 64-разрядный блок зашифрованного текста;
A - функция шифровки в режиме простой замены;
C1 и C2 - константы: C1 = 01010101h C2 = 01010104h;
Y(i) и Z(i) - 32-разрядные числа, которые определяются итеративно по формулам:

$$(Y(0), Z(0)) = A(S) \quad (14)$$

$$(Y(i), Z(i)) = (Y(i-1)\ [+]C2,\ Z(i-1)\ \{+\}C1\ ), \quad (15)$$

где S - 64-разрядная синхропосылка.

Синхропосылка не является секретным элементом шифра и передается вместе с зашифрованным сообщением. При дешифровке отделяется синхропосылка и формируется вектор (Y(0), Z(0)) за формулой (44).

64-разрядный блок открытого текста T(i) вычисляется по формуле:

$$T(i)= Г(i) \square\square Ш(i) \quad (16)$$

где Г(i) - блок дешифрующей гаммы, что определяется уравнениями (42) и (45).

Режим гаммирования

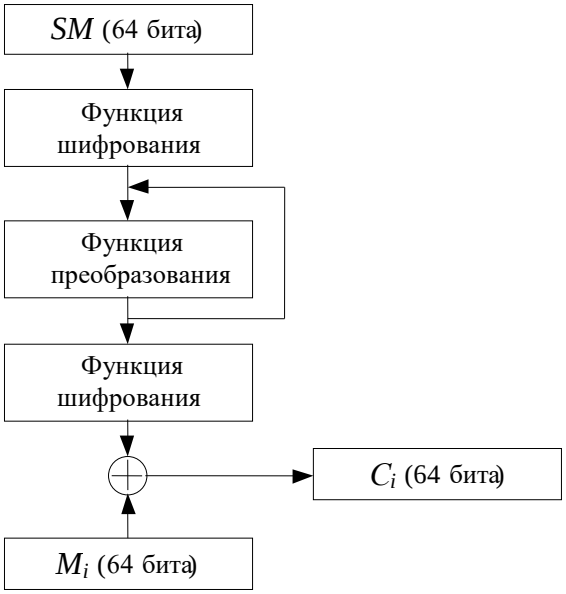


Рисунок 3. Работа алгоритма ГОСТ 28147-89 в режиме гаммирования с обратной связью

Открытые данные T, которые подлежат шифровке, разбиваются на блоки T(j) длиной 64 бита.

Уравнение шифровки данных в этом режиме может быть представлено в виде:

$$Ш(1)= A(S) \square\square T(1) \quad (17)$$

$$Ш(i)= A(Ш(i-1)) \square\square T(i)= Г(i) \square\square\square\square\square \quad \square 18)$$

где Ш(i) - 64-разрядный блок зашифрованного текста;
A - функция шифровки в режиме простой замены;
S - 64-разрядная синхропосылка.
Уравнение дешифровки в режиме гаммирования с обратной связью может быть представлено уравнениями:

$$T(1)= A(S) \square\square Ш(1) \quad (19)$$

$$T(i)= A(Ш(i-1)) \square\square Ш(i)= Г(i) \square\square Ш(i). \quad (20)$$

Режим гаммирования с обратной связью

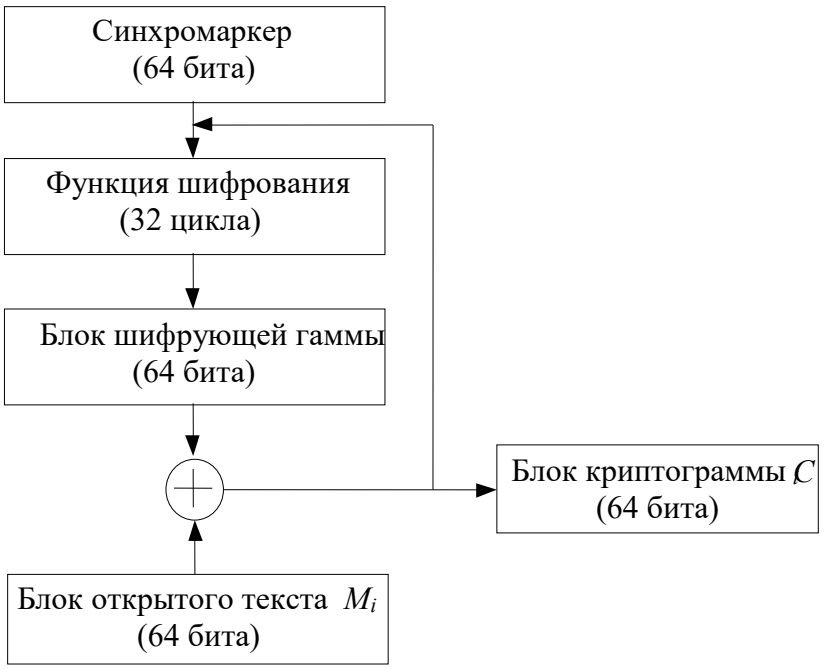


Рисунок 4.Работа алгоритма ГОСТ 28147-89 в режиме выработки имитовставки.

Для получения имитовставки открытые данные T, которые подлежат шифровке, разбиваются на блоки T(j) длиной 64 бита. Первый блок T(1) подвергается преобразованию, которое отвечает первым 16 циклам алгоритма шифровки в режиме простой замены, причем в качестве ключа выработки имитовставки используется ключ шифровки данных. Полученное 64-разрядное число складывается по модулю 2 со вторым блоком открытых данных T(2). Результат суммирования подвергается преобразованию, которое отвечает первым 16 циклам алгоритма шифровки в режиме простой замены.

Последний блок T(m), при необходимости дополненный к 64-разрядному числу нолями, складывается по модулю 2 с результатом работы на (m-1) -м шаге и зашифровывается. Из полученного 64-разрядного числа выделяется отрезок Ip длиной p битов, который является хеш-функцией открытых данных (имитовставкой). Значение параметру p определяется исходя из необходимости обеспечения необходимой вероятности обмана.

При расшифровке аналогично формируется имитовставка I’p, которая сравнивается с имитовставкой Ip, которая содержится в принятом сообщении. В случае несовпадения полученное сообщение считается подмененным.

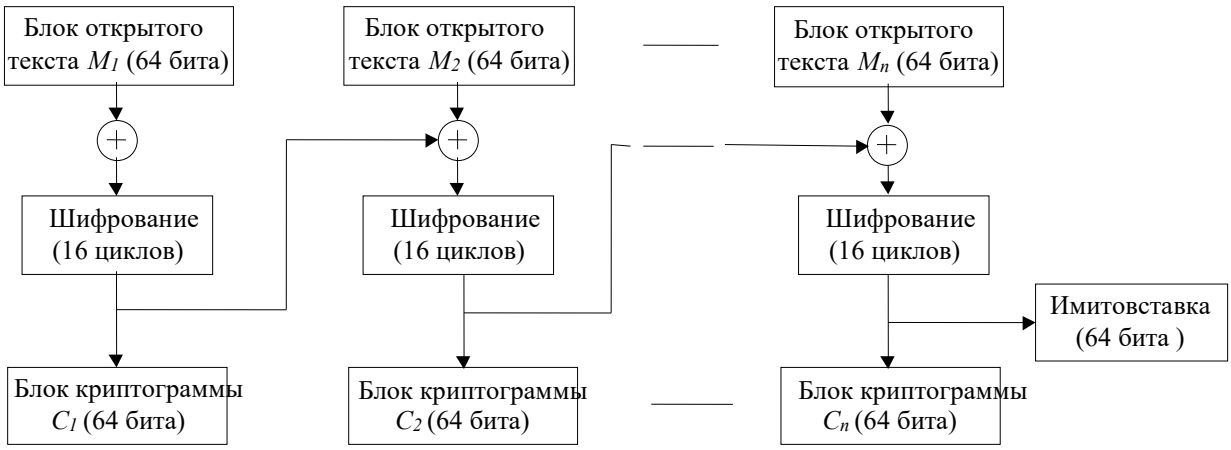


Рисунок 5. Режим выработки имитовставки

Порядок выполнения работы

1. Одиночная и двойная перестановка по ключу

Программа Transposition выполняет одиночную и двойную перестановку по ключу произвольного текстового сообщения.

Окно программы состоит из двух частей (вкладок), каждая из которых является интерфейсом для выполнения отмеченных алгоритмов.

Одиночная перестановка по ключу

Для выполнения шифровки необходимо выполнить следующие действия:

1. Снять флажок „Розшифрувати”.

2. Ввести открытый текст в поле „Відкритий текст”. При этом программа автоматически заполнит таблицу.

3. Перетянуть столбцы таблицы в таком порядке, чтобы ключ шифровки, который отображается в поле „Ключ”, равнялся необходимому ключу шифровки. Программа при этом проведет автоматическую перестановку букв и запишет полученный шифртекст в поле „Шифртекст”.

Для выполнения расшифровки необходимо выполнить следующие действия:

1. Установить флажок „Разшифровать”.

2. Ввести шифртекст в поле „Шифртекст”. При этом программа автоматически заполнит таблицу.

3. Ввести ключ расшифровки в поле „Ключ”. Программа при этом автоматически заполнит верхнюю строку таблицы.

4. Перетянуть столбцы таблицы в таком порядке, чтобы цифры в верхней строке таблицы располагались в верном порядке (например „1234”). Программа при этом проведет автоматическую перестановку букв и запишет полученный открытый текст в поле „Открытый текст”.

Дополнительные опции:

−возможность сохранить в текстовый файл таблицы шифровки-расшифровки.

Двойная перестановка по ключу

Для выполнения шифровки необходимо выполнить следующие действия:

5. Снять флажок „Расшифровать”.

6. Ввести открытый текст в поле „Открытый”. При этом программа автоматически заполнит таблицу.

7. Перетянуть столбцы и строки таблицы в таком порядке, чтобы ключи шифровки, которые отображаются в полях „Ключ 1” и „Ключ 2”, равнялись необходимым ключам шифровки. Программа при этом проведет автоматическую перестановку букв и запишет полученный шифртекст в поле „Шифртекст”.

Для выполнения расшифровки необходимо выполнить следующие действия:

1. Установить флажок „Разшифровать”.

2. Ввести шифртекст в поле „Шифртекст”. При этом программа автоматически заполнит таблицу.

3. Ввести ключи расшифровки в поля „Ключ 1” и „Ключ 2”. Программа при этом автоматически заполнит верхнюю строку и левый столбик таблицы.

4. Перетянуть столбцы и строки таблицы в таком порядке, чтобы цифры в верхней строке и в левом столбце таблицы располагались в верном порядке (например „1234”). Программа при этом проведет автоматическую перестановку букв и запишет полученный открытый текст в поле „Открытый”.

Дополнительные опции:

– возможность сохранить в текстовый файл таблицы шифровки-расшифровки.

2. Шифр Виженера

Программа Viginer выполняет шифровку с помощью шифра Вижинера.

Окно программы состоит из следующих частей:

– строка главного меню;

– поле для ввода открытого текста при шифровке или шифртекста при расшифровке;

– поле, в котором отображается результат шифровки-расшифровки.

Для выполнения шифровки необходимо выполнить следующие действия:

1. Ввести открытый текст в поле „Исходный текст”.
2. Ввести алфавитный ключ шифровки-расшифровки.
3. Выбрать алфавит шифровки.
4. В меню „Правка” выбрать пункт „Зашифровать”. При этом результат шифровки отобразится в нижнем текстовом поле.

Для выполнения расшифровки необходимо выполнить следующие действия:

1. Ввести шифртекст в поле „Исходный текст”.

2.Ввести алфавитный ключ шифровки-расшифровки.

3.Выбрать алфавит, который использовался при шифровке.

4.В меню „Правка” выбрать пункт „Расшифровать”. При этом результат расшифровки отобразится в нижнем текстовом поле.

Для редактирования списка алфавитов выполнить такие действия:

– отредактировать строку алфавита;

– нажать „+”, чтобы добавить этот алфавит в список;

– если необходимо, удалить некоторые алфавиты кнопкой „–”;

Дополнительные опции (меню „Правка”):

– возможность загрузки начального текста из файла и сохранения конечного текста в файл;

– возможность автоматического переноса текста из поля конечного текста в поле начального текста;

– возможность автоматической фильтрации начального текста;

– возможность автоматического перевода начального текста в верхний или нижний регистры;

3. Стандарт шифрования данных (DES)

Программа DES выполняет шифровку с помощью шифра DES (Data Encryption Standard).

Окно программы состоит из следующих частей:

– поле для ввода ключа шифровки;

– поле для ввода открытого текста при шифровке

– поле, в котором отображается результат шифровки;

– поле, в котором отображается процесс шифровки;

Для выполнения шифровки необходимо выполнить следующие действия:

1. Ввести ключ шифровки в поле „Ключ”, или генерировать его случайно („Выработать случайный ключ”).

2. Ввести открытый текст в поле „Открытый текст”, или генерировать его случайно („Выработать случайный текст”).

3. Нажать кнопку „Шифровать”. При этом результат шифровки отобразится в текстовом поле „Шифртекст”, а процесс шифровки – в нижнем текстовом поле;

4.Исследовать изменения сообщения в каждом раунде шифровки в зависимости от вида ключа и открытого текста.

4. Алгоритм шифрования ГОСТ 28147-89

Программа GOST выполняет шифровку с помощью алгоритма, который является частью стандарта криптопреобразования ГОСТ 28147-89.

Окно программы состоит из следующих частей:

– 8 полей для ввода ключа шифровки (общая длина – 256 бит);

– поле для ввода открытого текста при шифровке

– поле, в котором отображается результат шифровки;

– поле, в котором отображается процесс шифровки;

Для выполнения шифровки необходимо выполнить следующие действия:

1. Ввести ключ шифровки в поле „Ключ”, или генерировать его случайно („Случайный ключ”).

2. Ввести открытый текст в поле „Открытый текст”, или генерировать его случайно („Случайное сообщение”).

3. Нажать кнопку „Шифровать”. При этом результат шифровки отобразится в текстовом поле „Шифртекст”, а процесс шифровки – в нижнем текстовом поле.

4.Исследовать изменения сообщения в каждом раунде шифровки в зависимости от вида ключа и открытого текста.

Программа AGOSTA обеспечивает шифровку и дешифровку с помощью алгоритма ГОСТ 28147-89 в различных режимах работы.

1. Сформируйте произвольный текстовый файл.

2. Выполните шифрование этого файла с помощью команды:

AGOSTA -oe <режим> <входной файл> <выходной файл> <знак удаления>

Параметр <режим> задает режим алгоритма шифровки и может принимать численные значения от 1 до 4.

Параметр <знак удаления> может принимать значение:

0 - не удалять начальный файл;

1 - удалять начальный файл.

После запуска программы необходимо ввести произвольный пароль. Этот пароль будет использоваться для генерации сеансового ключа.

Пример:

AGOSTA -oe -1 x.txt x.sec 0

3. Выполните расшифровку файла с помощью команды:

AGOSTA -d <режим> <вхідний файл> <вихідний файл> <ознака видалення>

После запуска программы необходимо ввести тот же пароль, что и для шифрования.

Пример:

AGOSTA -d -1 x.sec x1.txt 0

4. Выполните шифрование и расшифрование, используя все 4 режима алгоритма ГОСТ.

5. Повторите п.4, но при этом внесите изменения в зашифрованный файл (начиная с 32-го символа). Определите, как при этом изменится расшифрованный файл. Поясните, почему произошли именно такие изменения.

6. Повторите п.4, но при этом внесите изменения в открытый текст. Определите, как при этом изменится зашифрованный файл. Поясните, почему произошли именно такие изменения.

5. Содержание отчета.

Отчет должен содержать:

– цель исследований и программу работы;

– короткое описание используемого блочного симметричного шифра;

– процедуры, которые реализовывают шифрование-расшифрование.

– выводы о целесообразности использования изученных режимов в различных ситуациях.

6. Контрольные вопросы.

1. Дайте общую характеристику алгоритму шифровки ГОСТ 28147-89.
2. Дайте характеристику режимов алгоритма ГОСТ 28147-89.
3. Как обеспечивается подлинность при использовании алгоритма ГОСТ 28147-89?
4. Пояснить работу алгоритма ГОСТ в режиме простой замены.
5. Пояснить работу алгоритма ГОСТ в режиме поточного шифрования (гаммирования).
6. Пояснить работу алгоритма ГОСТ в режиме поточного шифрования (гаммирования) с обратном связью.
7. Пояснить работу алгоритма ГОСТ в режиме выработки имитовставки.
8. Вычислить безопасное время и расстояние единственности для алгоритмов ГОСТ и DES.
9. Проведите сравнительный анализ алгоритмов ГОСТ и DES.
10. Дайте характеристику ключевых систем алгоритмов ГОСТ и DES.
11. Сравните текущие и блочные криптосистемы. Назовите их основные достоинства и недостатки.
12. Сформулируйте предложения по применению алгоритма шифровки ГОСТ 28147-89 для цифровой подписи.

Лабораторная работа №31-32

Тема: Исследование процедуры формирования и проверки электронной цифровой подписи на основе ассиметричного алгоритма RSA

Цель работы:

- закрепить на практике теоретические знания по особенностям реализации и использования КСЗИ (криптографических систем защиты информации) на базе криптопреобразований, стойкость которых основывается на сложности проблемы факторизации (разложения на простые сомножители) больших чисел;
- научиться оценивать стойкость криптосистем подобного типа в зависимости от условий реализации и использования алгоритмов криптопреобразований.

Теоретическая часть

— ознакомиться с материалом лекций по данной теме и, при необходимости, с указанной дополнительной литературой;

— повторить общую характеристику ключевой системы для криптосистем изучаемых типов;

— изучить основные методы и алгоритмы криптопреобразований (прямых и обратных) для систем рассматриваемых типов;

— ознакомиться с описанием лабораторной работы и ее программным обеспечением;

— подготовить бланк отчета согласно разделу "Содержание отчета" (предпочтительно в электронном виде);

— подготовить ответы на контрольные вопросы.

Выполнение криптопреобразований по схеме RSA

Шифрование / расшифрование

Шифрование выполняется по следующему правилу:

$$C_i = M_i^E \bmod N,$$

где M_i — текущий блок исходного текста ($M_i < N$);

C_i — сформированная криптограмма (зашифрованный блок текста);

E — ключ шифрования (при направленном шифровании является открытым);

N — открытый модуль криптопреобразований.

Соответственно, расшифрование выполняется по следующему правилу:

$$M_i = C_i^D \bmod N,$$

где D — ключ расшифрования (при направленном шифровании является конфиденциальным).Формирование / проверка электронной цифровой подписи

Формирование цифровой подписи состоит из следующих этапов.

1) Создать открытую подпись (большого целое число) $V < N$, содержащую избыточность — как правило, информацию об исходном подписываемом тексте **M** (сжатый образ текста — значение криптографической хеш – функции **H (M)**), а также о некоторых параметрах систем формирования подписи и управления ключевыми структурами и т.п. (в зависимости от требований конкретной реализации).

Например, в простейшем случае открытая цифровая подпись может состоять из следующих полей:

A_1	A_2	S	L_M	H (M)	$\{T_1, \ldots, T_k\}$
Адрес	Адрес	Идентификационные данные	Длина подписываем	Контрольная сумма	Временные метки

отправителя	получателя	отправителя (подпись)	ого сообщения	(значение хеш-функции)	

В качестве временных меток могут использоваться, например, время формирования подписи (для защиты от ранее переданных сообщений, от перестановки подписанных сообщений и т.п.), время действительности ключа (или время ввода его в действие и время окончания срока действия), время «жизни» подписи и т.д. на усмотрение разработчика КСЗИ.

2) Сформировать ЦП (непосредственно закрытую подпись):

$\mathbf{S = V^{E} \bmod N}$,

где **V** — исходное значение открытой подписи (большое число **V < N**);

S — формируемая закрытая цифровая подпись;

E — конфиденциальный ключ формирования подписи;

N — открытый модуль криптопреобразований.

3) Отправить получателю подписанное сообщение — **{M, S}**. При необходимости обеспечения не только аутентификации, но и конфиденциальности сообщение **M** может дополнительно зашифровываться по какому-то из алгоритмов и отправляться получателю в виде пары **{C, S}**.

Исходное /(или зашифрованное) сообщение	Закрытая ЦП
M / (C)	**S**

При этом формирование ЦП **S** выполняется до шифрования (то есть по параметрам исходного **M**, а не зашифрованного текста **C**). Если для выполнения шифрования используются симметричные алгоритмы (как известно, с точки зрения вычислительной сложности они лучше несимметричных алгоритмов шифрования), то симметричный ключ шифрования можно, при необходимости, передавать вместе с подписанным сообщением в зашифрованном виде (по схеме несимметричного направленного шифрования). В этом случае прочитать сообщение и проверить его подлинность сможет только сторона, владеющая конфиденциальным ключом схемы направленного шифрования (легальный получатель). Очевидно, что при этом пары ключей для схем несимметричного шифрования и подписи не только не должны совпадать, но и не должны вычисляться для одного и того же модуля криптопреобразований **N**. То есть должно существовать два набора ключевых данных: для ЦП $\mathbf{\{(D_{ФЦП}, N_1)}$ — конфиденциальные ключевые данные для формирования подписи $\mathbf{, (E_{ПЦП}, N_1)}$ — открытые ключевые данные для проверки подписи } и для направленного шифрования $\mathbf{\{(D_{РШФ}, N_2)}$ — конфиденциальные ключевые данные $\mathbf{, (E_{ШФ}, N_2)}$ — открытые ключевые данные **}**, причем $\mathbf{N_1 \neq N_2}$.

В данной реализации лабораторной работы подписанный файл имеет следующий вид.

Исходное /(или зашифрованное) сообщение	Служебное поле	Закрытая ЦП	Служебное поле	Дополнительное служебное поле
M / (C)	**_RSA_DS_**	**S**	**_RSA_DS_**	

Проверка цифровой подписи состоит из следующих этапов.

1) Из полученного подписанного сообщения — $\mathbf{\{M^{*}, S^{*}\}}$ — выделить значение закрытой цифровой подписи $\mathbf{S^{*}}$.

Появление в обозначениях символа “ * ” означает, что в процессе пересылки по каналам связи (или хранения) значение подписанного текста и / или соответствующее ему значение цифровой подписи было модифицировано (случайно либо преднамеренно) либо подделано.

2) Восстановить значение открытой подписи:

$\mathbf{V^* = (S^*)^D \bmod N}$,

где $\mathbf{V^*}$ — восстанавливаемое значение открытой подписи (ОП) (большое число $\mathbf{V^* < N}$);

$\mathbf{S^*}$ — полученное значение закрытой цифровой подписи (возможно, модифицированное либо поддельное);

D — открытый ключ проверки подписи;

N — открытый модуль криптопреобразований.

Наличие символа "*" при значении восстановленной ОП означает, что оно может, в общем случае, не совпадать с исходным значением **V** открытой подписи, сформированным автором сообщения (на передающей стороне).

3) Проверить элементарную корректность избыточной информации, содержащейся в восстановленной открытой подписи $\mathbf{V^*}$. Например, сравнить с параметрами полученного текста $\mathbf{M^*}$: сравнить значение хеш – функции **H = H (M)**, восстановленное из $\mathbf{V^*}$ и значение, вычисленное на приемной стороне по тому же общеизвестному алгоритму хеширования из полученного текста $\mathbf{M^*}$ — то есть $\mathbf{H^* = H(M^*)}$; сравнить длину текста, время его формирования и другие подобные значения полей восстановленной открытой подписи $\mathbf{V^*}$. А также сравнить информацию, содержащуюся в восстановленной открытой подписи $\mathbf{V^*}$ с параметрами систем формирования подписи и управления ключевыми структурами (проверить соответствие допустимому диапазону) и т.п. При обнаружении каких – либо несоответствий полученная ЦП $\mathbf{V^*}$ считается поддельной. То есть делается вывод о том, что при передаче / хранении сообщение $\mathbf{M^*}$ (или ЦП $\mathbf{V^*}$) было модифицировано (случайно либо преднамеренно) или является поддельным — то есть произошло нарушение целостности и / или подлинности исходного подписанного сообщения **{M, S}** ($\mathbf{M^* \neq M}$ или подпись **S** сформирована для несанкционированного сообщения **M**).

4) При корректности всех проверок делается вывод о том, что с определенной степенью вероятности (зависящей от выбора параметров реализации криптосистемы) полученное подписанное сообщение $\mathbf{\{M^*, S^*\}}$ является целостным и подлинным (то есть совпадает с исходным сформированным сообщением $\mathbf{\{M^*, S^*\} = \{M, S\}}$).

Порядок выполнения работы

1. Сформировать ключевую систему.

Сформировать ключевые данные с использованием программы **ZIB_Lb4.exe**, выбрав пункт меню "**Генерация ключевых данных → RSA → Для простых чисел общего вида … ".** При этом в диалоговом окне «Формирование файлов открытых (E, N) и конфиденциальных (D, N) ключевых данных» установить длину модуля криптопреобразований равной 512 (бит).

При закрытии данного диалога по кнопке <OK> сформированные ключевые данные записываются в двоичные файлы в подкаталоги, прописанные в соответствующем файле конфигурации (формат см. в **Ошибка! Источник ссылки не найден.**)

2. Изучить процесс формирования RSA - цифровой подписи, используя демонстрационно – обучающую программу (ZIB_Lb5.exe**).**

1) Выбрать пункт меню "**Демонстрация → RSA → Цифровая подпись → Подписать файл … " .**

2) В появившемся диалоговом окне выбрать файл, для которого будет далее выполняться формирование цифровой подписи.

Лучше для наглядности выбрать текстовый файл, так как подпись добавляется в конец файла и может нарушить формат представления файлов других типов. (Пример возможного формата добавляемой закрытой подписи, используемого в данной лабораторной работе, приведен в 0)

Если выбранный файл уже был ранее подписан тем же типом подписи, то программа выдаст соответствующее предупреждение и запрос о целесообразности проведения дальнейших действий. (Использование повторной ЭЦП в рамках данной учебной программной модели не желательно, хотя и допустимо.)

По выбранному файлу в случае его успешного прочтения будут сформированы отдельные поля открытой цифровой подписи: длина файла, хеш – значение и т.п. Для формирования хеш-значения в данной лабораторной работе используется алгоритм хеширования SHA – 160 (один из вариантов алгоритмов из стандарта FIPS 180 - 2).

3) В появившемся диалоговом окне "Демонстрация формирования цифровой подписи для файла" заполнить недостающие поля цифровой подписи (например, адреса и идентификационные данные).

Обратить особое внимание на следующие моменты:

- состав полей открытой цифровой подписи **V** (см. подразд. 0);
- содержимое отдельных полей (пояснить назначение и порядок формирования каждого из них);
- постоянное изменение одного из полей в области временных меток;
- размеры отдельных полей открытой ЦП;
- общий размер структуры открытой ЦП (чем он определяется, как определяются размеры отдельных полей).

При закрытии демонстрационного диалога по кнопке <OK> выполняется добавление в подписываемый файл закрытой цифровой подписи **S**, сформированной по открытой подписи **V** с использованием конфиденциальных ключевых данных. При этом на экране появляется соответствующее сообщение.

4) Ознакомиться со структурой подписанного файла (внести в отчет).

Пример возможного варианта формата добавляемой закрытой подписи, используемого в данной лабораторной работе, приведен в подразд. 0.

3. Изучить процесс проверки RSA - цифровой подписи, используя демонстрационно – обучающую программу (ZIB_Lb5.exe**).**

1) Выбрать пункт меню "**Демонстрация → RSA → Цифровая подпись → Проверить подпись файла … " .**

При выполнении проверки ЦП чтение открытых ключевых данных (ключевой пары **{D, N }** автора сообщения из базы / файла открытых ключей) выполняется автоматически из файла, указанного в используемом файле конфигурации, согласно полю **ID** s в подписанном файле.

2) В появившемся диалоговом окне выбрать файл, для которого необходимо проверить подпись (файл, подписанный на текущих ключах, указанных в файле конфигурации).

4. Исследовать функционирование программной модели цифровой подписи при имитации возникновения нарушений в канале связи (при передаче подписанных сообщений). Для этого выполнить нижеприведенные пункты заданий.

Примечание. При выполнении нижеприведенных пунктов исследования не рекомендуется выполнять модификацию подписанного файла с использованием редакторов типа Word, WordPad и т.п., поскольку они некорректно сохраняют некоторые двоичные символы, содержащиеся в поле S электронной цифровой подписи (можно использовать только редакторы, корректно обрабатывающие произвольные коды). Это ограничение вызвано тем, что в текущем варианте демонстрационной программы пока не подключена кодировка radix - 64.

1) Попытаться выбрать имя неподписанного файла. Пояснить (внести в отчет), за счет чего была обнаружена ошибка.

2) **Изучить возможности обнаружения несанкционированных изменений (подделок) посредством проверки ЦП**. Для этого внести следующие типы изменений в подписанный файл и попытаться повторно выполнить проверку ЦП. Пояснить (внести в отчет), за счет чего был обнаружен каждый тип ошибки.

(1) Добавить один (или более) символ в основной текст подписанного сообщения (в информационную часть).

(2) Удалить один (или более) символ из основного текста подписанного сообщения (из информационной части).

(3) Модифицировать один (или более) символ из основного текста подписанного сообщения (из информационной части). («Модификация» подразумевает сохранение прежней длины сообщения.)

(4) Модифицировать один (или более) символ из поля закрытой цифровой подписи (находящейся между зарезервированными служебными полями, см. формат подписанного файла в подразд. 0). («Модификация» подразумевает сохранение прежней длины поля закрытой ЦП.)

Обратить внимание, как при этом нарушении изменяются значения в восстановленных полях открытой ЦП (даже при изменении хотя бы одного бита в закрытой ЭЦП **S**).

Содержание отчета

В отчете (оформленном в электронном виде индивидуально каждым студентом) должно быть представлено следующее.

Тема и цель лабораторной работы.

Результаты и выводы по ним согласно требованиям к порядку выполнения работы.

Контрольных вопросы

1) Что такое конфиденциальность.
2) Что такое шифрование, для каких целей оно может использоваться, какие функции СЗИ позволяет реализовать (полностью либо частично — в комбинации с другими механизмами КСЗИ).
3) Что такое аутентификация.
4) Пояснить, что подразумевается под понятиями “контроль целостности” и “контроль подлинности”.
5) Что такое цифровая подпись.
6) Для каких целей может использоваться ЦП, какие функции КСЗИ (криптографических систем защиты информации) она позволяет реализовать (полностью либо частично — в комбинации с другими механизмами КСЗИ).
7) Что является конфиденциальными, а что открытыми ключевыми данными в RSA – схеме направленного шифрования.
8) Привести и пояснить математические соотношения для выполнения шифрования / дешифрования по RSA – схеме.
9) Показать математически, что соотношение для расшифрования практически всегда корректно восстанавливает исходный зашифрованный текст.
10) Что является конфиденциальными, а что открытыми ключевыми данными в RSA – схеме цифровой подписи.
11) Пояснить, как формируются открытая и закрытая цифровая подпись по RSA – схеме. Привести вариант возможной структуры цифровой подписи и пояснить назначение отдельных полей. Привести примеры типов атак, для защиты от которых предназначены эти поля открытой подписи.

Лабораторная работа №33-34

Тема: Исследование схемы разделения секрета

Цель работы:

- изучить требования, сущность, методы построения, порядок анализа свойств, принципы реализации и основные сферы применения протоколов разделения секрета.

Теоретическая часть

Очень важной областью криптографии, которая интенсивно развивается в последние годы, являются специфические протоколы, которые получили название схем (протоколов) разделения секрета. По своей сущности схемы разделения секрета являются многосторонними протоколами, основной функцией которых является установка ключей или паролей. При этом под установкой ключей понимается процесс или прикладной протокол, в результате выполнения которого общая тайна (ключ, пароль) становится доступной объектам или субъектам информационной технологии, что позволяет им выполнять криптографическую защиту с необходимым качеством. Сначала элементы разделения секрета применялись для создания резервных копий ключей и обеспечения криптографической стойкости систем.

Схемы разделения секрета нашли также применение и для совместного управления критическими технологиями и процессами. В таком управлении могут принимать n объектов или субъектов.

Идея разделения секрета заключается в том, что общая тайна делится на n частей, которые называют долями (частицами) тайны. При объединении к≤n частиц тайны используются предельные схемы разделения секрета, которые позволяют установить ключ при согласии не меньше чем к – объектов и субъектов

Предельные схемы разделения секрета.

В предельной схеме общий секрет разделяется на n частей. Однако восстановление секрета может быть выполнено по $k \le n$ частных секретов. В этой схеме доверенная сторона также формирует общий секрет S и из него вычисляет частные секреты S_i каждого объекта. При этом на S_i налагаются также ограничения, чтобы каждые k объектов, представив k истинных секретов S_i могли бы вычислить общий секрет S. Более того, если при вычислении S используется $k+v$ частных секретов, то v из них могут быть ошибочными или поддельными, а k настоящих все равно обеспечивают формирование общего секрета. Подчеркнем, что на этапе разделения и использования секрета значения S_i должны распространяться и сохраняться с обеспечением целостности и конфиденциальности. Кроме того, в такой схеме ни одна группа, которая знает только $k-1$ частичных секретов, восстановить S не может.

Построение известной пороговой схемы Аде Шамира базируется на интерполяции, полинома, и на том факте, что одномерный полином $f(x)$ степени $k-1$ над полем Галуа уникально задается по k точкам. Полиномы могут быть заданы над p-ичным расширенным полем. При этом коэффициенты a_i полинома $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}$ задаются над полем $GF(p)$ как элементы поля Z_p. Основными параметрами такой схемы являются числа (k,n), где k есть минимальное число частей секрета, с использованием которых может быть восстановлен общий секрет, а n- общее число частей секрета, причем $1 \le k \le n$.

Коэффициенты a_i определяются или задаются числом n частей секрета. Потом случайным образом формируется общий секрет S, который должен быть разделен на части секрета S_i $i = \overline{1,n}$. Предлагаемая схема должна быть такой, чтобы любые k объектов или субъектов, объединив свои k частных секретов могли однозначно восстановить общий секрет S. При этом все части секрета S_i являются конфиденциальными, и на протяжении их жизненного цикла должна быть обеспечена их целостность.

При выполнении приведенных выше требований и условий пороговая схема разделения секрета Шамира реализуется таким способом.

1.Формируется большое простое число P, которое больше допустимого $P_Д$, то есть

$P > P_o$.

2.Формируется случайным образом общий секрет S, который является элементом поля, то есть целое S удовлетворяет условию:

$1 < S < p$

3. Случайно формируется $k-1$ коэффициентов полинома $f(x)$, которые объявляются конфиденциальными.

4. В качествах a_0 принимается значение общего секрета S, то есть $a_0 = S$.

5. Доверенная сторона разделяет общий секрет, вычисляя части секрета $S_i = f(i)$, где числовой идентификатор или номер каждого из объектов или субъектов, причем $1 \le i \le p-1$. Разделение секрета может заключаться в присвоении каждому из объектов или субъектов уникального случайного идентификатора.

6.Все части секрета S_i транспортируются и устанавливаются с обеспечением конфиденциальности и целостности.

В дальнейшем мы рассмотрим отдельно алгоритм контроля подлинности каждой из частей секрета.

Восстановление общего секрета производится на основе использования не менее k целостных и настоящих частей секрета, $k + v \le n$ частей секрета, не более чем v из которых могут быть сформированы объектом или субъектом злоумышленником или подделаны. Эти v и менее частных секретов с нарушенной целостностью отбрасываются и не учитываются при выработке общего секрета. Восстановление общего секрета выполняется в следующем порядке.

1.Каждый из объектов (субъектов) передает и/или устанавливает частный секрет $S_i = f(i)$ в доверенное устройство выработки общего секрета с обеспечением конфиденциальности, целостности и подлинности.

2.Доверенное устройство контролирует целостность и подлинность частных секретов, если эта функция реализована в схеме разделения секрета, а затем выбирает из них k настоящих.

3.По k значениям $f(i_i),..., f(i_k)$ в доверенном устройстве производится восстановление $f(x)$ с использованием интерполяционной формулы Лагранжа:

$$f(x) = \sum_{e=1}^{k} f(i_e) \prod_{j \ne l} \frac{x - i_j}{i_e - i_j} \ . \qquad (1.1)$$

Общий секрет формируется в виде

$S = a_0 = f(0)$.

В дальнейшем S может использоваться в качестве ключа, пароля, общего секрета и др.

Таким образом, выработка общего секрета в доверенном (исполнительном) устройстве производится на основе восстановления полинома, то есть вычисление вектора коэффициентов $a_1, a_2, ..., a_{k-1}$, а затем определения общего секрета как $S = a_0 = f(0)$

Проведенный анализ показывает [2], что свойства предельной схемы разделения секрета Шамира позволяют построить протокол с нулевыми знаниями. При соответствующем выборе параметров знания $k-1$ значения $f(i_i),..., f(i_{k-1})$ не дают никакой информации об общем секрете. Его стойкость базируется на интерполяционной формуле Лагранжа, а также зависит от длины модуля преобразований P и длин S_i-х частиц секрета. Рассмотрим возможные атаки на схему Шамира. Основной задачей атак является определение общего секрета $S = a_0$. Значение a_0 можно определить непосредственно через определение значений частных секретов $f(l_1),..., f(l_k)$. Если $S = a_0 = f(0)$ формируется доверенной стороной случайно, то сложность атаки типа "грубая сила" по определению a_0 можно оценить через вероятность P_0 ее осуществления

$$P_0 = \frac{1}{p-2} \approx \frac{1}{p} = p^{-1}. \qquad (1.2)$$

Сложность атаки "грубая сила" по определению a_0 через значение $f(i_1), f(i_2),..., f(i_k) \in GF(p)$ можно оценить как

$$P_f = \left(\frac{1}{(p-1)^k} \right) = (p-1)^{-k} \approx p^{-k}. \qquad (1.3)$$

Сравнение выражений показывает, что более лучшая есть атака по непосредственному определению a_0 . Сложность этой атаки зависит только от величины модуля p . Если p есть открытый общесистемный

параметр, известный криптоаналитику, то сложность атаки можно определить также через безопасное время

$$\text{Тб} = T_{\text{б}} = \frac{I_0}{\zeta K} \approx \frac{P}{\zeta K}, \qquad (1.4)$$

где $I_0 \approx p$ есть число попыток подбора значения a_0 с вероятностью 1; ζ - производительность криптоаналитической системы; $K = 3{,}1 \cdot 10^7$ сек/рік - количество секунд в год. При этом условии $T_б$ измеряется в годах. Если a_0 должен быть определен с вероятностью P_q, то $T_б$ с такой вероятностью определяется из соотношения

$$T_б^{\text{P}_q} = \frac{p}{\zeta K} \text{P}_q . \qquad (1.5)$$

В табл. 1 приведены значения $I_0 = p$ и $T_б$ при $\zeta_k = 10^{12}$ и 10^{16} вар/сек. (в знаменателе).

Сложность восстановления общего секрета схемы Аде – Шамира

Таблица 1

p	2^{64}	2^{128}	2^{256}	2^{512}	2^{1024}
$T_б$ (лет) $P_д = 1$	$\frac{6*10^{-1}}{6*10^{-5}}$	$\frac{10^{19}}{10^{15}}$	$\frac{4*10^{58}}{4*10^{54}}$	$\frac{10^{134}}{10^{130}}$	$\frac{10^{288}}{10^{284}}$
$T_д$ (лет) $P_д = 10^{-16}$	$\frac{6*10^{-17}}{6*10^{-21}}$	$\frac{10^{3}}{10^{-1}}$	$\frac{4*10^{42}}{4*10^{38}}$	$\frac{10^{118}}{10^{114}}$	$\frac{10^{272}}{10^{268}}$

Анализ данной таблицы показывает, что применения значения $T_б$ для криптографических преобразований достигаются уже при величине модуля p порядка 2^{256}. При длине модуля $p = 2^{256}$ вероятность, с которой может быть осуществленный криптоанализ с $\text{P} = 10^{-16}$ и производительностью криптоаналитической системы 10^{16}, безопасное время составляет не менее 10^{38} лет. Потому в перспективных схемах разделения секрета величины модулей p должны составлять порядок $2^{256} – 2^{512}$.

Основными свойствами пороговой схемы Ади-Шамира являются следующие:

1.Независимость. При знании любых $k-1$ и менее частиц секрета S_i все значения общего секрета S остаются ровновероятными и теоретически могут выбираться из интервала $0 \le S \le p-1$.

2.Отсутствие не доказанных допущений. В отличие от вероятностно стойких схем схема А. Шамира не базируется ни на каких недоказанных допущениях (например, сложности решения таких задач как факторизация модуля, пребывание дискретного логарифма и т.д.).

3.Расширение с появлением новых пользователей. Это свойство заключается в том, что новые части секрета могут быть вычислены и распределены без влияния на уже существующие части.

4.Идеальность, под которой понимается тот факт, что все части общего секрета и сам общий секрет имеют одинаковый размер и могут принимать значение над полем $GF(p)$ с равной вероятностью.

Особенностью предельной схемы деления секрета является то, что она требует выполнение модульных операций над большим полем, сложность которых имеет характер полинома. Кроме того доверенное устройство должно иметь возможность контролировать целостность и подлинность частей секрета перед выработкой общего секрета.

Восстановление секрета.

Если доверенное устройство не является злоумышленником, то протокол восстановления общего секрета выполняется таким способом.

Каждый объект A_j посылает доверенному устройству свою часть секрета S_i, обеспечивая его целостность и конфиденциальность. Доверенная сторона может проверить целостность всех принятых S частей секрета, используя специальный алгоритм.

Части секрета, которые не прошли проверку, не используются. Если честных объектов, что предоставили частные секреты, не менее чем K, то доверенное устройство получает не менее чем K частей общего секрета и может восстановить общий секрет, используя схему Шамира, описанную выше.

Примеры решения задач.

Задача 1.

Разделение секрета в системе осуществляется по схеме Шамира с параметрами к=5. Необходимо:

1) выбрать размер поля GF(p), над которым осуществляется разделение секрета
2) сформировать общий секрет
3) вычислить частичные секреты
4) сформировать общий секрет, получив частичные, используя интерполяционную формулу Лагранжа.

Решение

1) сначала формируем простое число $P > P_{äîï}$, например для наглядности P=37;

2) порождаем случайно общий секрет, что является элементом поля GF(p), то есть $1 \le S \le P-1$. Например S=29;

3) поскольку к=5, то формируем случайно к-1=4 коэффициентов a_1, a_2, a_3, a_4. Например $a_4 = 27$. В качестве a_0 выбираем $a_0 = S_0$.

4) Присваиваем каждому из объектов или субъектов числовые значения идентификаторов $i_1 = 16,\ i_2 = 3,\ i_3 = 24,\ i_4 = 35,\ i_5 = 7.$

5) Полином f(x) имеет вид: $f(x) = (a_0 + a_1x^1 + a_2x^2 + a_3x^3 + a_4x^4) \bmod P$, подставим у него числовые данные, получим: $f(x) = (29 + 7x^1 + 31x^2 + 18x^3 + 27x^4) \bmod 37$

Находим частичные секреты, подставив в полином $x = i_{1.....4}$, то есть

$$f(16) = (29 + 7*16 + 31*16^2 + 18*16^3 + 27*16^4) \bmod 37 = 93 \bmod 37 = 19 \bmod 37$$

$$f(3) = (29 + 7*3 + 31*3^2 + 18*3^3 + 27*3^4) \bmod 37 = 79 \bmod 37 = 5 \bmod 37$$

$$f(24) = (29 + 7*24 + 31*24^2 + 18*24^3 + 27*24^4) \bmod 37 = 108 \bmod 37 = 34 \bmod 37$$

$$f(35) = (29 + 7*35 + 31*35^2 + 18*35^3 + 27*35^4) \bmod 37 = 94 \bmod 37 = 20 \bmod 37$$

$$f(7) = (29 + 7*7 + 31*7^2 + 18*7^3 + 27*7^4) \bmod 37 = 115 \bmod 37 = 4 \bmod 37$$

Таким образом: $S_1 = f(i_1) = 19$,

$S_2 = f(i_2) = 5$,

$S_3 = f(i_3) = 34$,

$S_4 = f(i_4) = 20$,

$S_5 = f(i_5) = 4$.

В дальнейшем $S_0 = 29$ устанавливается в доверенное средство в качестве общего секрета. Частичные секреты $S_{1...5}$ распространяются в системе с обеспечением целостности и подлинности.

Пусть необходимо восстановить общий секрет, причем все объекты (субъекты) согласны. В этом случае каждый из них передает свой секрет в доверенное устройство, обеспечив их целостность, подлинность и конфиденциальность.

В средстве, которому доверяют, осуществляется восстановление f(x). Для этого используется интерполяционная формула Лагранжа $f(x) = \sum_{e=1}^{k} f(i_e) \prod_{j \ne e} \left(\frac{x - i_j}{i_e - i_j}\right)$. Подставив в нее мгновенные числовые значения, получим:

$$f(x) = \left(19 * \frac{x-3}{16-3} * \frac{x-24}{16-24} * \frac{x-35}{16-35} * \frac{x-7}{16-7} + 5 * \frac{x-16}{3-16} * \frac{x-24}{3-24} * \frac{x-35}{3-35} * \frac{x-7}{3-7} + \right.$$

$$+ 34 * \frac{x-16}{24-16} * \frac{x-3}{24-3} * \frac{x-35}{24-35} * \frac{x-7}{24-7} + 20 * \frac{x-16}{35-16} * \frac{x-3}{35-3} * \frac{x-24}{35-24} * \frac{x-7}{35-7} +$$

$$\left. + 4 * \frac{x-16}{7-16} * \frac{x-3}{7-3} * \frac{x-24}{7-24} * \frac{x-35}{7-35} = \frac{19}{17784} * (x^2 - 27x + 35) * (x^2 - 5x + 23) + \right.$$

$$+ \frac{5}{34944} * (x^2 - 3x + 14) * (x^2 - 5x + 23) + \frac{34}{-31416} * (x^2 - 19x + 11) * (x^2 - 5x + 23) +$$

$$\left. + \frac{20}{187264} * (x^2 - 19x + 11) * (x^2 + 6x + 20) + \frac{4}{-17136} * (x^2 - 19x + 11) * (x^2 + 15x + 26) = \right.$$

(проведем подсчеты обратных элементов:

$17784 = 24 \bmod 37 \quad \frac{37}{24} = 1 + \frac{13}{24}; \frac{24}{13} = 1 + \frac{11}{13}; \frac{13}{11} = 1 + \frac{2}{11}; \frac{11}{2} = 5 + \frac{1}{2}; \frac{2}{1} = 2. \quad k = 4$

$a_0 = 1,\ a_1 = 2,\ a_2 = 3,\ a_3 = 17 \qquad y = 17 \bmod 37.$

$34944 = 16 \bmod 37 \quad \frac{37}{16} = 2 + \frac{5}{16}; \frac{16}{5} = 3 + \frac{1}{5}; \frac{5}{1} = 5. \quad k = 2$

$a_0 = 2,\ a_1 = 7, \qquad y = 7 \bmod 37.$

$-31416 = 34 \bmod 37 \quad \frac{37}{34} = 1 + \frac{3}{34}; \frac{34}{3} = 11 + \frac{1}{3}; \frac{3}{1} = 3. \quad k = 2$

$a_0 = 1,\ a_1 = 12, \qquad y = 12 \bmod 37.$

$187264 = 7 \bmod 37 \quad \frac{37}{7} = 5 + \frac{2}{7}; \frac{7}{2} = 3 + \frac{1}{2}; \frac{2}{1} = 2. \quad k = 2$

$a_0 = 5,\ a_1 = 16 \qquad y = 16 \bmod 37.$

$-17136 = 32 \bmod 37 \quad \frac{37}{32} = 1 + \frac{5}{32}; \frac{32}{5} = 6 + \frac{2}{5}; \frac{5}{2} = 2 + \frac{1}{2}; \frac{2}{1} = 2. \quad k = 3$

$a_0 = 1,\ a_1 = 7,\ a_2 = 15 \qquad y = (-1)^3 * 15 \bmod 37. = 22 \bmod 37.$

)

$= (19 * 17 * (x^4 - 5x^3 + 23x^2 - 27x^3 + 24x^2 + 8x + 35x^2 + 10x + 28) +$

$+ 5 * 7 * (x^4 - 5x^3 + 23x^2 - 3x^3 + 15x^2 + 5x + 14x^2 + 4x + 26) +$

$+ 34 * 12 * (x^4 - 5x^3 + 23x^2 - 19x^3 + 21x^2 + 7x + 11x^2 + 19x + 31) +$

$+ 20 * 16 * (x^4 + 6x^3 + 20x^2 - 19x^3 - 3x^2 - 10x + 11x^2 + 29x + 35) +$

$+ 4 * 22 * (x^4 + 15x^3 + 26x^2 - 19x^3 + 11x^2 + 24x + 11x^2 + 17x + 27)) \bmod 37 =$

$= (27x^4 + 24x^3 + 31x^2 + 5x + 16 + 35x^4 + 16x^3 + 7x^2 + 19x + 22 + x^4 + 13x^3 +$

$+ 18x^2 + 26x + 31 + 24x^4 + 21x^3 + 6x^2 + 12x + 26 + 14x^4 + 18x^3 + 6x^2 + 19x + 8) \bmod 37 =$

$= (27x^4 + 18x^3 + 31x^2 + 7x + 29) \bmod 37.$

В итоге был восстановлен начальный полином, где f(0) и есть общий секрет.

Задача 2

Следующая задача формулируется таким же образом, как и предыдущая, но с той разницей, что при построении общего секрета один частичный секрет был передан неправильно, или специально был искажен. Например, это был секрет под номером 5, то есть, пусть он стал равняться 2. Тогда при построении начального полинома по формуле Лагранжа, получим:

$$f(x) = (19 * \frac{x-3}{16-3} * \frac{x-24}{16-24} * \frac{x-35}{16-35} * \frac{x-7}{16-7} + 5 * \frac{x-16}{3-16} * \frac{x-24}{3-24} * \frac{x-35}{3-35} * \frac{x-7}{3-7} +$$

$$+ 34 * \frac{x-16}{24-16} * \frac{x-3}{24-3} * \frac{x-35}{24-35} * \frac{x-7}{24-7} + 20 * \frac{x-16}{35-16} * \frac{x-3}{35-3} * \frac{x-24}{35-24} * \frac{x-7}{35-7} +$$

$$+ 2 * \frac{x-16}{7-16} * \frac{x-3}{7-3} * \frac{x-24}{7-24} * \frac{x-35}{7-35} = \frac{19}{17784} * (x^2 - 27x + 35) * (x^2 - 5x + 23) +$$

$$+ \frac{5}{34944} * (x^2 - 3x + 14) * (x^2 - 5x + 23) + \frac{34}{-31416} * (x^2 - 19x + 11) * (x^2 - 5x + 23) +$$

$$+ \frac{20}{187264} * (x^2 - 19x + 11) * (x^2 + 6x + 20) + \frac{2}{-17136} * (x^2 - 19x + 11) * (x^2 + 15x + 26) =$$

(проведем подсчеты обратных элементов:

$17784 = 24 \bmod 37 \quad \frac{37}{24} = 1 + \frac{13}{24};\ \frac{24}{13} = 1 + \frac{11}{13};\ \frac{13}{11} = 1 + \frac{2}{11};\ \frac{11}{2} = 5 + \frac{1}{2};\ \frac{2}{1} = 2.\ \ k = 4$

$a_0 = 1,\ a_1 = 2,\ a_2 = 3,\ a_3 = 17 \qquad y = 17 \bmod 37.$

$34944 = 16 \bmod 37 \quad \frac{37}{16} = 2 + \frac{5}{16};\ \frac{16}{5} = 3 + \frac{1}{5};\ \frac{5}{1} = 5.\ \ k = 2$

$a_0 = 2,\ a_1 = 7, \qquad y = 7 \bmod 37.$

$-31416 = 34 \bmod 37 \quad \frac{37}{34} = 1 + \frac{3}{34};\ \frac{34}{3} = 11 + \frac{1}{3};\ \frac{3}{1} = 3.\ \ k = 2$

$a_0 = 1,\ a_1 = 12, \qquad y = 12 \bmod 37.$

$187264 = 7 \bmod 37 \quad \frac{37}{7} = 5 + \frac{2}{7};\ \frac{7}{2} = 3 + \frac{1}{2};\ \frac{2}{1} = 2.\ \ k = 2$

$a_0 = 5,\ a_1 = 16 \qquad y = 16 \bmod 37.$

$-17136 = 32 \bmod 37 \quad \frac{37}{32} = 1 + \frac{5}{32};\ \frac{32}{5} = 6 + \frac{2}{5};\ \frac{5}{2} = 2 + \frac{1}{2};\ \frac{2}{1} = 2.\ \ k = 3$ **)**

$a_0 = 1,\ a_1 = 7,\ a_2 = 15 \qquad y = (-1)^3 * 15 \bmod 37. = 22 \bmod 37.$

$$= (19 * 17 * (x^4 - 5x^3 + 23x^2 - 27x^3 + 24x^2 + 8x + 35x^2 + 10x + 28) +$$
$$+ 5 * 7 * (x^4 - 5x^3 + 23x^2 - 3x^3 + 15x^2 + 5x + 14x^2 + 4x + 26) +$$
$$+ 34 * 12 * (x^4 - 5x^3 + 23x^2 - 19x^3 + 21x^2 + 7x + 11x^2 + 19x + 31) +$$
$$+ 20 * 16 * (x^4 + 6x^3 + 20x^2 - 19x^3 - 3x^2 - 10x + 11x^2 + 29x + 35) +$$
$$+ 2 * 22 * (x^4 + 15x^3 + 26x^2 - 19x^3 + 11x^2 + 24x + 11x^2 + 17x + 27)) \bmod 37 =$$
$$= (27x^4 + 24x^3 + 31x^2 + 5x + 16 + 35x^4 + 16x^3 + 7x^2 + 19x + 22 + x^4 + 13x^3 +$$
$$+ 18x^2 + 26x + 31 + 24x^4 + 21x^3 + 6x^2 + 12x + 26 + 7x^4 + 9x^3 + 3x^2 + 28x + 4) \bmod 37 =$$
$$= (20x^4 + 9x^3 + 28x^2 + 16x + 25) \bmod 37.$$

как мы видим, получив хотя бы один неверный частичный ключ, невозможно восстановить порождающий полином, а вместе с ним и общий ключ.

Порядок выполнения работы

1. Изучить теоретический материал, предоставленный в разделах 1.2, 1.3 данной лабораторной работы.

2. С помощью программы Rezmir.exe:

а) сформировать большое простое число P (модуль);

б) сформировать общий секрет S (простое число);

в) ввести количество идентификаторов;

г) сформировать коэффициенты полинома;

д) сформировать числовые идентификаторы.

(Все данные, отображаемые в окне программы REZMIR.EXE, а также содержимое файла res . txt, поместить в отчет).

3. После выполнения пункта 1.5.2 перенести сформированные файлы (модуль, частичные секреты, числовые идентификаторы) в каталог программы Sec_compon;

4. С помощью программы Sec_compon сформировать общий секрет, выполнив все требования, которые будут указаны в этой программе.

(В отчет поместить данные, отображаемые в окне программы SEC_COMPON.EXE и содержимое файла „secret").

5. Изменить (в соответствующем файле) одну из частей общего секрета (или идентификатора), с помощью программы Sec_compon снова сформировать общий секрет и убедиться, что вновь сформированный общий секрет отличается от сформированного ранее.

(В отчет поместить содержимое модифицированного файла; данные, отображаемые в окне программы SEC_COMPON.EXE и содержимое файла „secret").

Содержание отчета

- цель исследований и программу работы;
- основные формулы для применения криптографического протокола разделения секрета;
- сформированные данные;
- выводы по работе.

Контрольные вопросы

1. Для чего предназначены и что обеспечивают протоколы разделения секрета?
2. В чем суть и какие свойства имеет пороговая схема Шамира разделения секрета?
3. Какие и каким образом формируются общесистемные параметры схемы Шамира разделения секрета?
4. В чем сущность этапов построения пороговой схемы Шамира разделения секрета?
5. Дайте характеристику протоколу восстановления секрета в схеме Шамира.
6. Что позволяет интерполяционная формула Лагранжа и какие данные для нее необходимы?
7. На чем базируется стойкость схемы Шамира?
8. Обоснуйте и выберите параметры схемы разделения секрета.

Лабораторная работа 35-36

Тема: Изучение средств выявления каналов утечки информации на примере высокочувствительного сканирующего приемника AR-5000A «КВАДРАТ»

Цель работы :

- **ознакомится с основными характеристиками и возможностями высокочувствительного сканирующего приемника AR-5000A «КВАДРАТ»**

Порядок выполнения работы

- ознакомится с представленным материалом;
- ответить на контрольные вопросы;
- оформить отчет.

I. Сканирующие радиоприемники

В процессе контроля радиоэфира основными действиями являются поиск, обнаружение и прием требуемых радиосигналов. Возможности любого комплекса радиоконтроля, решающего эти задачи, определяются параметрами используемых в нем сканирующих радиоприемных устройств. По сути дела именно эти устройства являются одним из важнейших функциональных элементов такого комплекса. Следует отметить, что сканирующие приемники в руках злоумышленников могут служить разведывательным средством.

Сканирующие радиоприемники характеризуются следующими основными показателями:

• диапазоном принимаемых частот;
• чувствительностью;
• избирательностью;
• параметрами сканирования (скоростью перестройки, полосами обзора и т.д.);
• используемым методом или методами, если они есть, обнаружения сигналов;
• видом принимаемых радиосигналов;
• оперативностью управления и возможностями его автоматизации;
• выходными параметрами (качество воспроизведения сигнала на выходе приемника, наличие выходов по промежуточной и низкой частоте, значения полос пропускания сигнала по этим частотам и т.д.);
• эксплуатационными параметрами (массогабаритные характеристики, требования по электропитанию, надежность, ремонтопригодность. удобство транспортировки и т.п.).

Представленные на отечественном рынке модели сканирующих приемников обычно удовлетворяют требованиям по диапазону и скорости сканирования для поиска радиомикрофонов или других источников радиоизлучения, не использующих режим быстрой перестройки рабочей частоты.

В то же время возможность обнаружения таких радиомикрофонов или способность контроля технически сложных каналов радиосвязи зависят не только от параметров сканирования радиоприемника, но и от наличия в составе комплекса других средств, обеспечивающих решение подобных задач. В качестве таких средств в настоящее время все чаще используются специализированные комплекты программного обеспечения. В этих условиях особое значение приобретает способность сканирующего радиоприемника эффективно работать в составе автоматизированного комплекса радиоконтроля под управлением персонального компьютера.

С этой целью рядом зарубежных и российских компаний производителей были разработаны так называемые «компьютерные» радиоприемники, специально ориентированные на обеспечение эффективного взаимодействия с ЭВМ. Конструктивно такие приемники выполняются либо в виде плат, встраиваемых в ISA-слот компьютера, либо в виде отдельных модулей, подключаемых к компьютеру через порты COM, LPT или PCMCIA. Благодаря такому решению обеспечивается высокая скорость обмена информацией между радиоприемником и компьютером, а отсутствие дополнительных внешних органов управления позволяет достичь небольших значений массогабаритных параметров приемника.

1. Сканирующий приемник AR5000-A

Сканирующий приемник AR5000-A в составе многоканального комплекса радиоконтроля «Квадрат» (далее «комплекс») предназначен для выявления, оценки параметров и регистрации несанкционированных радиоизлучений, а также организации постоянного контроля за радиообстановкой. Комплекс Квадрат может использоваться в мобильных и стационарных системах радиоконтроля. Комплекс реализует метод пространственно-разнесенных антенн для выявления,

оценки параметров и идентификации источников радиоизлучений в контролируемых помещениях здания на частотах 40-3000 МГц с возможностью расширения полосы контроля до 5960 МГц.

Рис.1 Сканирующий приемник AR5000-A

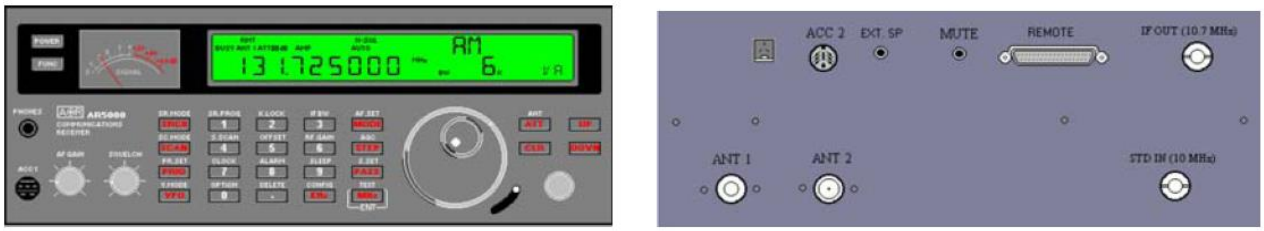


Рис.2 Передняя и задняя панель приемника

2. Состав комплекса радиоконтроля «Квадрат»

В типовой комплект поставки комплекса входят:

1) радиоприемное устройство с адаптером питания;
2) векторный процессор радиосигналов RT2000 S;
3) специальное программное обеспечение «RT-2060»;
4) широкополосные антенны VHF-30 или VHF-30A;
5) антенный коммутатор на 4 канала.

Дополнительное оборудование (поставляется по отдельному заказу):

6) дополнительные антенны VHF-30 или VHF-30A;
7) активные антенны типа АА-2012 или АА-2013;
8) генератор прицельной помехи СМ/J мощностью 0,25 или 1 Вт;
9) имитатор стандартных сигналов СМ/Т;
10) СВЧ конвертер со специальным программным обеспечением (3000-5960 МГц);
11) конвертор проводных линий LS1000 (600Гц-10МГц).

3. Технические характеристики комплекса.

Радиочастотная часть:

Частотный диапазон:	
-анализатор проводных линий	0,0006-10 МГц
-ВЧ анализатор	40 - 3000 МГц
-СВЧ конвертер	3000 - 5960 МГц
Чувствительность -	не хуже 2 мкВ [-101 dBm]
Динамический диапазон	70дБ
Разрешение:	
-в режиме анализа	0,1 кГц
-в режиме обнаружения	2 кГц
Скорость сканирования	до 100 МГц/с
Полоса обзора в режиме экспресс-анализа	0,1…50 МГц
Полоса параллельного обзора	200 кГц
Мин. длительность обнаруживаемого импульса	1.5 с.

Отображаемые характеристики сигнала –
временные, частотные, комплексные (вектор).

Общие параметры:

Габариты сумки-укладки 540х340х320 мм
Масса (для стандартной комплектации) 16 кг

Эксплуатационные параметры:

Диапазон рабочих температур +5…+35 °С

RT 2060 (CM3000) является программной оболочкой комплекса радиоконтроля **КВАДРАТ**, предназначенного для решения различных задач радиоконтроля и анализа электромагнитной обстановки, в том числе для автоматического обнаружения, идентификации, локализации и нейтрализации подслушивающих устройств, передающих данные по радиоканалу и проводным линиям.

Комплекс может использоваться для организации как стационарных, так и мобильных постов радиоконтроля. Высокая скорость обзора, чувствительность и разрешающая способность позволяют ему быстро и надежно выявлять и оценивать параметры любых источников сигналов и радиоизлучений в диапазоне частот от 0.6кГц до 5960 МГц.

Комплекс оснащается базовым программным обеспечением для автоматического обнаружения, анализа, классификации и регистрации сигналов и может поставляться с дополнительными аппаратными и программными средствами, расширяющими возможности комплекса в различных условиях эксплуатации.

Комплекс радиоконтроля КВАДРАТ **использует несколько пространственно разнесенных антенн для** выявления, оценки параметров и идентификации источников радиоизлучений в контролируемых помещениях зданий, а также для организации постоянного контроля за радиообстановкой и поиска несанкционированных излучений на частотах от 40 до 3000 МГц.

Программные средства пространственной классификации отбирают из всего множества обнаруженных сигналов только те, которые излучаются внутренним источниками, что значительно ускоряет и упрощает работу оператора при поиске каналов утечки информации.

Система располагает векторным анализатором **для исследования спектральных, временных и модуляционных характеристик радиосигналов в реальном времени**, а также автоматическим регистратором для записи в **память компьютера фонограмм демодулированных радиосигналов.**

Типовая схема построения распределенной системы радиомониторинга объекта на базе комплекса «Квадрат» имеет следующий вид:

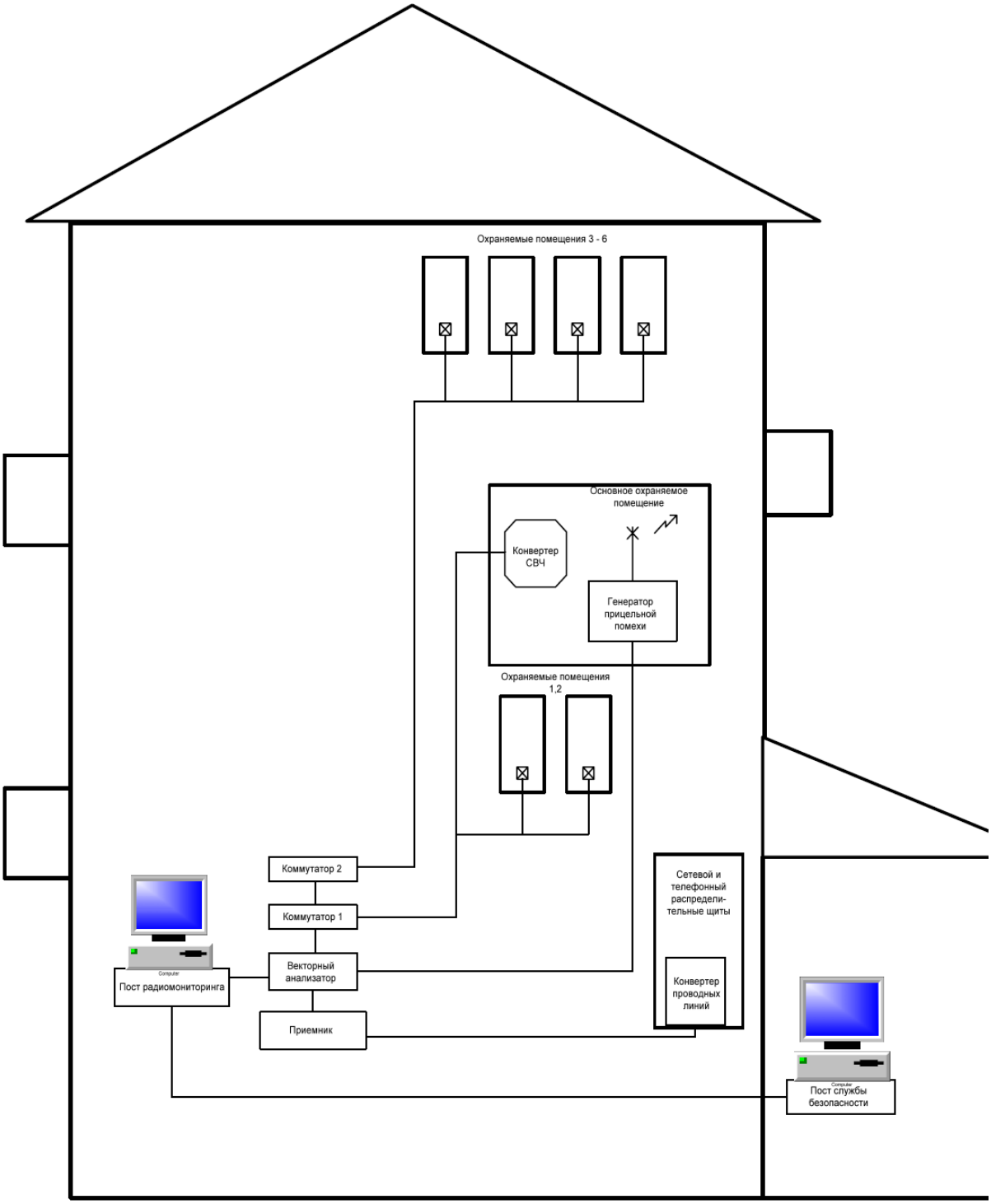


Рис.3 Типовая схема построения распределенной системы радиомониторинга объекта на базе комплекса «Квадрат»

В минимальной комплектации для решения задач контроля в диапазоне до 3ГГц комплекс поставляется с двумя приемными широкополосными антеннами и комплектом ВЧ кабелей (два кабеля 15 метров). Возможно расширение комплектации комплекса дополнительной широкополосной антенной. Широкополосные антенны предназначены для приема сигналов в диапазоне частот от 40 МГц до 3 ГГц. Антенны выполнены в пыле – влагозащищенном исполнении.

Диаграмма направленности широкополосной приемной антенны в горизонтальной плоскости представлена на следующем рисунке.

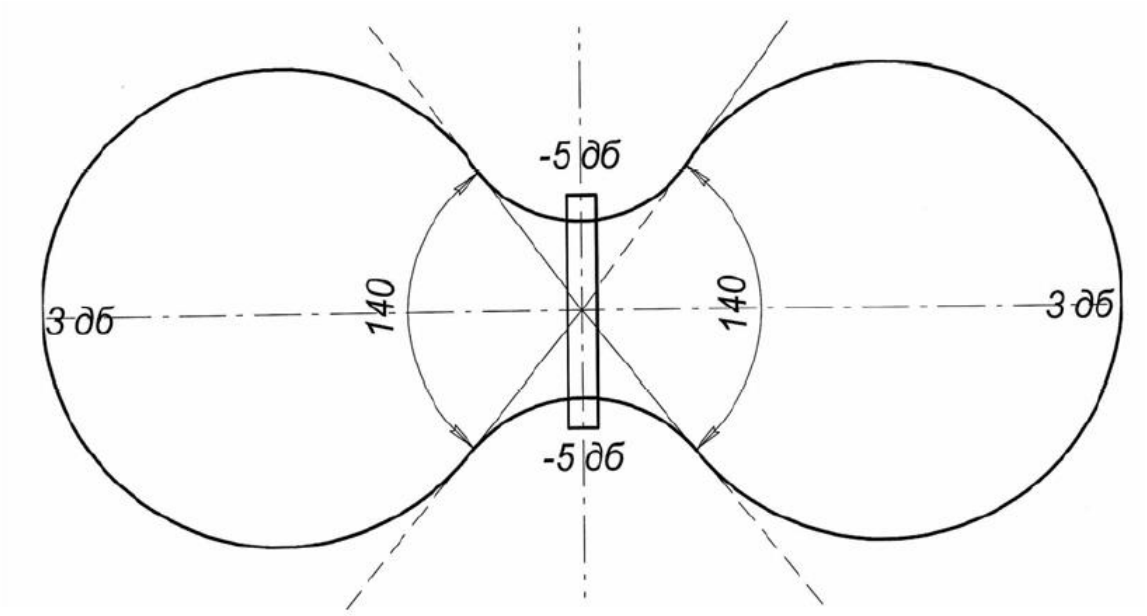


Рис.4 Диаграмма направленности антенны VHF-30

4. Возможности программы.

Программа функционирует в одном из четырех базовых режимов.

- **В режиме сбора данных** он с высокой скоростью последовательно просматривает заданный диапазон радиочастот, обнаруживает все сигналы, мощность которых превышает установленные пороговые уровни, выполняет анализ спектра и измерение параметров обнаруженных сигналов и помещает полученные сведения в базу данных управляющей программы. В процессе сбора данных о радиосигналах на экран компьютера выводятся спектральные панорамы и спектрограмма, отображающие радиообстановку в исследуемой области частот за определенный промежуток времени.

- **В режиме обработки данных радионаблюдения** управляющая программа классифицирует обнаруженные сигналы в соответствии с установленными оператором критериями. Этот процесс позволяет отобрать из всего множества сигналов, хранящихся в базе данных и отражающих результаты работы обнаружителя за все время наблюдений, только те, которые представляют для оператора непосредственный интерес. В частности, пространственный классификатор делит все обнаруженные сигналы на две группы: излучаемые внешними источниками, расположенными на значительном удалении от контролируемой зоны, и локальные, создаваемые внутри таких зон.

Пространственный классификатор существенно ускоряет выявление нелегальных радиопередатчиков и других источников утечки информации по радиоканалу из внутренних помещений зданий даже в условиях сильной загрузки радиодиапазона внешними станциями.

По классификационным признакам программа создает сокращенный список обнаруженных сигналов. В режиме сбора данных после заданного числа циклов обзора могут автоматически выполняться операции обработки и отображение списка обнаруженных сигналов.

- **Режим анализа обнаруженных сигналов** используется для автоматического или ручного исследования спектральных, временных и модуляционных характеристик обнаруженных сигналов или отдельных участков радиодиапазона. В этом режиме возможна также ручная регистрация демодулированных сигналов через звуковую плату компьютера.

- **В режиме автоматической регистрации** программа выполняет обнаружение, классификацию и автоматическую регистрацию тех сигналов, которые отвечают заданным классификационным признакам.

Автоматизированный комплекс ***КВАДРАТ может использоваться для проведения следующих работ:***

- оперативной проверки помещений, электросети, телефонных линий и других коммуникаций с целью поиска устройств негласной передачи информации по радиоканалу или проводным линиям;
- постоянного контроля рабочего места руководителя, отдельных кабинетов или всего здания на наличие источников несанкционированных излучений, в том числе устройств с дистанционным включением или кратковременной работой, а также вносимых на время проведения совещаний, переговоров и других конфиденциальных мероприятий;
- выявления каналов утечки информации от средств оргтехники, связи и другой аппаратуры;
- круглосуточного контроля электромагнитной обстановки в помещении (помещениях) и решения общих задач радиоконтроля;
- управления генератором прицельной помехи СМ/J, с помощью которого возможно подавление нелегальных и подозрительных источников радиоизлучений во время проведения совещаний, переговоров и других конфиденциальных мероприятий.

Контрольные вопросы

1. Виды средств обнаружения радиозакладных устройств.
2. Перечислите основные устройства выявления побочных электромагнитных излучений.
3. Перечислите известные Вам программно-аппаратные комплексы для измерения ПЭМИН.
4. Типовой состав автоматизированных комплексов радиомониторинга.
5. Технические возможности комплексов радиомониторинга.
6. Какие характеристики электромагнитного поля определяются в выявленных побочных электромагнитных излучениях?
7. В каких расчетах используются характеристики электромагнитного поля побочных электромагнитных излучений?
8. В чем принципиальное отличие между программно-аппаратным комплексом радиомониторинга на основе сканирующего приемника и программно-аппаратным комплексом по оценке ПЭМИН?

Лабораторная работа 37

Обнаружение приборов наблюдения и оптических приборов

Цель работы: 1. Ознакомление студентов с работой аппаратуры определения оптических приборов и видеокамер.

2. Краткие теоретические сведения по принципам обнаружения.

3.Практическая работа на обнаружителе видеокамер.

Принцип обнаружения оптических приборов

Как правило, все подготовительные разведывательные действия террористического характера выполняются с применением разнообразных систем наблюдения (оптико-механических, телевизионных, ночного видения и прочих).

Одним из немногих демаскирующих признаков применения террористами и преступниками оптических приборов наблюдения, прицеливания и видения является их оптический контраст.

Активное применение обнаружителей оптических устройств дает возможность упредить действия террористов и преступников, которые могут привести к серьезным человеческим и материальным потерям и, кроме того, позволяет выиграть время для обеспечения реальной безопасности. Дальность обнаружения современных обнаружителей оптических устройств варьируется от 100 до 2500м.

Обнаружение оптических прицельно-наблюдательных приспособлений обеспечивается за счет эффекта световозвращения или «обратного блика». Этот эффект возникает, когда оптическое устройство освещается узконаправленным пучком света по оси оптического устройства или близко к ней и показан на рис. 2.

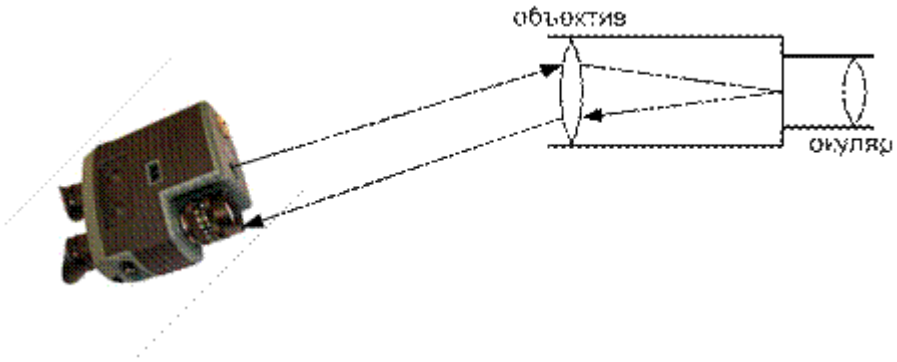


Рис. 2. Принцип действия обнаружителя оптических устройств

Яркость отраженного (световозвращающего) луча, как правило, на несколько порядков выше яркости диффузных вторичных источников, то есть непосредственно объектов, техники и местных предметов. Эффект будет возникать независимо от конструкции прицела и от того, что находится за ним. Свойства приборов позволяют обнаруживать оптическое и кино-фотонаблюдение, даже если оно ведется из-за тонированных или зеркальных стекол.

В зависимости от решаемой тактической задачи системы обнаружения оптических устройств делятся на стационарные и мобильные, портативные.

При установке систем на стационарных объектах предусмотрена организация работы как непосредственно с участием оператора, так и в автоматизированном режиме, с возможностью организации управления одновременно несколькими комплексами, с накоплением и передачей получаемой информации на удаленные пункты контроля.

Учитывая отсутствие у стационарных комплексов внешних отличий от стандартных охранно-телевизионных комплексов, исключается их ранняя идентификация со стороны террористов, ведущих наблюдение за объектом.

Мобильные и ручные приборы могут быть использованы в качестве эффективных средств предупреждения нападения, как на стационарные объекты, так и при организации надежной личной охраны руководителей и безопасности особо важных городских и загородных мероприятий.

В большинстве случаев обнаружители оптических устройств оснащаются инфракрасными лазерными излучателями и устройством наблюдения блика. Лазерные излучатели могут быть непрерывного и импульсного действия.

В приборах первого типа мощный лазер непрерывного действия, совмещенный с прибором ночного видения. Импульсные устройства совмещаются с инфракрасной видеокамерой и сложной логикой обработки сигнала, уменьшающей вероятность ложного обнаружения. Инфракрасная лазерная подсветка используется, в основном, с целью предотвращения обнаружения снайпером средств обнаружения оптических устройств.

Для эффективного поиска оптических устройств, работающих в видимом диапазоне, длина волны лазера должна быть максимально приближена к длине волны оптического диапазона, так как коэффициенты преломления волн различной длины в оптических приборах также различны. Поэтому используется лазер с длиной волны 700..900 нм. Такое концентрированное излучение очень слабо воспринимается глазом.

Примером обнаружителей оптических устройств является устройство «СПИН-2» (рис. 3.), предназначенное для дистанционного обнаружения оптических и оптико-электронных средств, прицелов, длиннофокусных объективов в условиях как интенсивного дневного, так и слабого ночного освещения на расстоянии до 1000 м. Прибор позволяет регистрировать оптико-электронные средства наблюдения в виде яркого блика на фоне подстилающей поверхности. Угол пеленга средств наблюдения соответствует углу поля зрения самих средств наблюдения. Визуализация наблюдаемых объектов осуществляется через встроенный электронный псевдобинокуляр.

Рис. 3. Средство обнаружения оптических устройств «СПИН-2»

Существуют портативные устройства, предназначенные для поиска скрытно установленных видео-фото-камер и других скрытых оптических устройств. Работают такие устройства по такому же принципу, однако имеются конструктивные отличия. Они обнаруживают оптику любого типа, даже если фотоаппарат или камера выключены, работают на расстояниях 5…20 м, что вполне достаточно, для того, чтобы обнаружить скрытно установленное в помещении оптическое устройство. В них используется видимый оптический диапазон, делая невозможным применение различного рода фильтров, т.к. фильтр сделает невозможным наблюдение скрытно установленным устройством.

Примером данного класса устройств является обнаружитель скрытых видеокамер «ВОРОН» (рис. 4), предназначен для быстрого обнаружения и определения местоположения скрытых (камуфлированных в различные предметы интерьера и одежды) микровидеокамер, в том числе с объективами типа «Pin-hole». Обнаружитель «ВОРОН» использует светодиодную подсветку целей, что гарантирует

безопасность эксплуатации и отсутствие вредного воздействия на человека (в отличие от лазерной подсветки). Дальность обнаружения объективов скрытых видеокамер типа Pin-Hole (ø 1 мм) составляет от 1 до 20 метров.

Средства обнаружения скрытых видеокамер

Сегодня технологии развиты до такой степени, что как только появляется новое приспособление для прослушки или скрытого видеонаблюдения, так тут же создаются средства, способные обнаружить и нейтрализовать такое приспособление. Устройства, позволяющие обеспечить безопасность какому-либо объекту, постоянно усовершенствуются, в них появляются новые функции и возможности для более эффективного использования. Точно так же происходит совершенствование устройств для обнаружения скрытых видеокамер. Многие злоумышленники потратили немало времени и сил для создания приборов скрытой фото- и видеосъемки, а также способов ночного наблюдения. Каждый раз создавалась видеокамера меньшего размера, чем ее предшественница, но с лучшими техническими характеристиками, благодаря которым улучшалось качество изображения. В зависимости от поставленных перед шпионом целей, выделяют видеокамеры проводные и беспроводные, работающие дистанционно или передающие изображение по радиоканалу. На сегодняшний момент, злоумышленник может установить камеру где угодно за считанные секунды - на одежде, на мебели, на стенах и так далее, а съемка будет проходить незаметно ни для кого. Пока известно три метода, применяя которые можно засечь скрытые камеры видеонаблюдения:
Применяется индикатор поля. Этот вариант подходит в том случае, когда информация передается по радиоканалу.
Применение оптических приспособлений. В этом случае лазерный луч прибора отражается от объектива скрытой видеокамеры.
Использование электромагнитного обнаружителя скрытых камер видеонаблюдения.

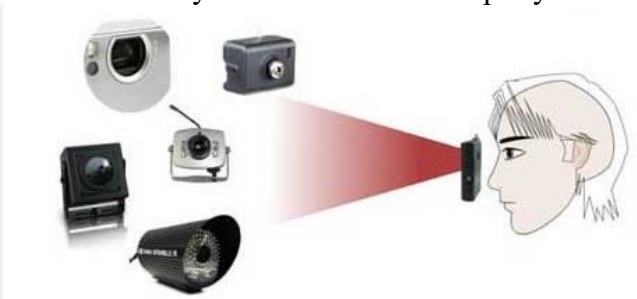
Радиолокация

Приборы, с помощью которых проводится поиск скрытых видеокамер, согласно первого способа являются самым обыкновенным индикатором поля. Такие приспособления очень часто используются на Западе. Они определяют все устройства, которые работают по радиоканалу и даёт возможность их заблокировать. Подобные технические средства, соответственно, позволяют обнаружить лишь беспроводные камеры, а так же другие типы жучков, использующих радиоканал для передачи данных.

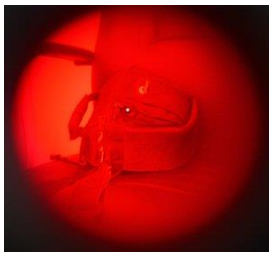
Оптическое исследование

Оптические приборы настроены на функционирование по принципу световозвращения. Объяснить это можно тем, что все приспособления для наблюдения и скрытые видеокамеры в том числе, оснащены ПЗС-матрицей или другим элементом обладающим светочувствительным свойством и если на него направить

лазерный луч, он отразится обратно к обнаружителю. Поэтому, для определения скрытой камеры достаточно направить лазерный луч прибора оптического типа на то место, где возможно размещена камера и будет заметен блик от светоотражающего элемента. Современные оптические приборы усовершенствованы до такой степени, что могут отсеивать излучения, исходящие от других приборов кроме камер. Для этих целей в устройства часто устанавливают ИК-пропускающий фильтр и четко подбирают параметры для лазерного луча.

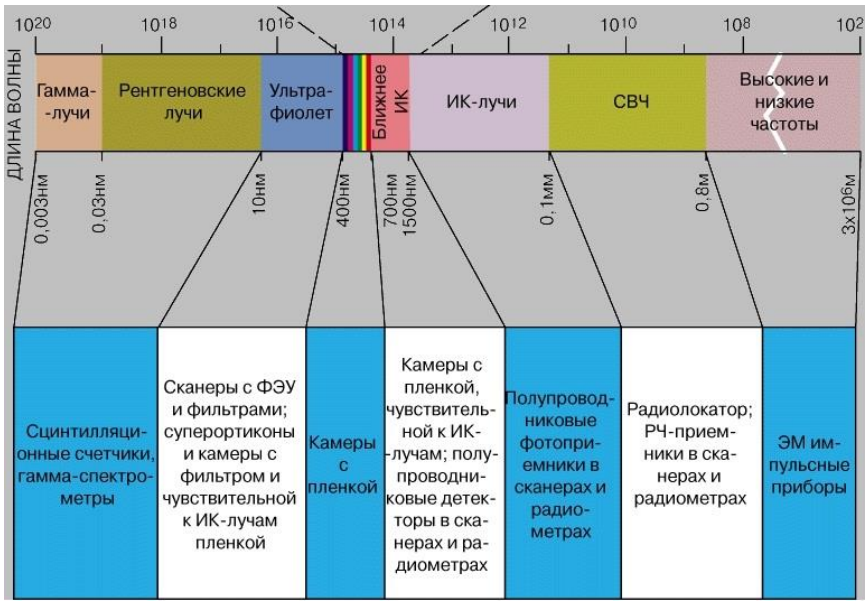


Оптический способ для обнаружения скрытых камер имеет как преимущества, так и недостатки. Таким способом можно легко засечь любое оптическое приспособление, будь то бинокль или снайперская винтовка. Однако, сегодня разработано множество светофильтров, способных отсеивать световые волны определенной длины.



Анализ электромагнитного поля

Третий способ, который позволяет зафиксировать скрытые камеры видеонаблюдения – это использование электромагнитных приспособлений (обнаружителей). Чтоб понять как они работают,необходимо знать из чего состоят сами камеры. В основной массе видеокамер установлена ПЗС-матрица в роли фотоприемника (приспособление, способное трансформировать световой сигнал в электрический). Такая матрица функционирует благодаря считывателю сигнала, то есть процессору, который впоследствии и создает сам видеосигнал. В процессоре есть осциллятор, он образует излучение на указанной частоте. Осциллятор способен излучать энергию лишь на маленькие расстояние, но имеет и другие излучения, которые состоят из гармоник главной частоты. Среди этих гармоник есть такие, которые способны очень хорошо проходить через корпус видеокамеры. Есть такой тип камер, который производит очень большое излучение на гармониках, а изображение записывается в память обнаружителя. Для каждой разновидности камер может быть свойственное только определённое излучение, поэтому обнаружитель содержит в памяти основные волновые характеристики большинства видеокамер, чтобы отсеивать волны, поступающие от сторонних электроприборов.

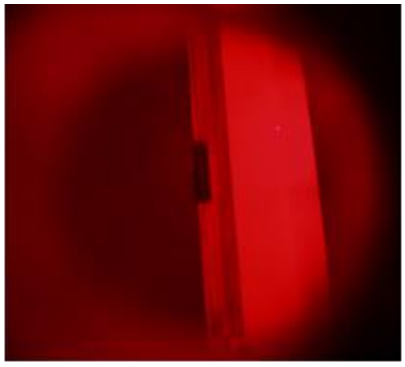


Как же происходит процесс обнаружения камер? Приспособление проводит анализ электромагнитных частот, которые находятся в периметре, и проводит сравнение с теми, которые заранее находятся в его памяти. Обнаружитель во время всего процесса делит полосу спектра, в котором находится осциллятор камеры, на небольшие сегменты, медленно повышая чувствительность. После чего обнаружитель определяет, что это за частота - скрытой камеры наблюдения или просто посторонняя помеха. Чтобы отсечь такого рода помехи, часто используют двойную верификацию и подтверждение. Встречаются участки, которые требуют тщательного анализа, бывает, проверка происходит четыре раза и только тогда удается определить, что за излучение - частота случайных помех или осциллятора скрытой камеры.

Особенности обнаружителей

Сегодня на рынке представлен широкий ассортимент видеокамер, самых разнообразных типов, обладающих несходными друг с другом техническими характеристиками. На территории России чаще всего используют видеокамеры PAL, на втором месте стоит камера типа NTSC, все остальные очень редко встречаются на практике. Систематизация образов в память камеры у всех разновидностей камер отличается. Есть камеры, в которых предусмотрена функция фиксирования образов, что находятся во встроенной памяти видеокамеры. А во многих других камерах эти образы сбрасываются. Частота осциллятора меняется от температуры воздуха в помещении и от электронных составляющих самого приспособления. Злоумышленники часто используют камеры дистанционного управления, в этом случае, после ее включения она прогревается и в обнаруженном ранее спектре ее уже не выявить. То есть через некий промежуток времени камера просто исчезает, и время на ее обнаружение было зря потеряно. Когда происходит процесс обнаружения скрытой камеры наблюдения, то на экране обнаружителя видеокамер показывается, какой уровень излучения исходит от анализированного участка, одни приборы настроены на отображение интегрального уровня излучения, а некоторые другие - отображают на дисплее наибольшую гармонику.

Видеокамера в галстуке



Видеокамера в стене лестничной площадки

Видеокамера в копировальном аппарате

Большего результата позволяет достичь использование второго варианта, так как в интегральном уровне может исчезнуть одна гармоника, попасть в зону, где ее невозможно зафиксировать. Это объясняется тем, что благодаря интерференции наложения волн их отражения значительно увеличиваются, а иногда и вовсе пропадают, из-за этого интегральный уровень полностью изменяется, по этой причине может произойти обнаружение скрытой видеокамеры в том участке, где ее и вовсе нет. И оптические приспособления, и электромагнитные способны зафиксировать наличие камеры в промежутке нескольких метров.

Оптический обнаружитель всех видов скрытых камер "Филин" предназначен для поиска спрятанных камер видео наблюдения. С помощью этого устройства Вы сможете без труда найти любые камеры вне зависимости от их состояния, включены они или выключены. Это могут быть проводные или беспроводные, скрытые или закамуфлированные.

Обнаружитель камер "Беркут", предназначен для поиска скрытых (закамуфлированных в различные предметы интерьера) видеокамер в не зависимости от их состояния. Находятся они во включенном или в выключенном состоянии. Обнаружитель скрытых видеокамер "Беркут" позволяет выявить как проводные камеры, так и видеокамеры, работающие по радиоканалу (беспроводные).

Дальность обнаружения

Дальность обнаружения оптических приборов зависит от того, какой тип подсветки установлен - непрерывная или импульсная; от возможности настройки по диоптриям; от того, какое зрение у человека, который проводит анализ помещения; от уровня освещения в исследуемом помещении и от многих других факторов.

При использовании электромагнитных обнаружителей, на дальность функционирования приспособления влияют тип камеры и то, каким образом от нее происходит излучение.

Если камера очень слабо излучает, то ее можно зафиксировать на расстоянии около трех метров.

Те камеры, которые настроены на высокое излучение, обнаруживаются в пределах 50 метров. Среднее излучение можно засечь в диапазоне 7-10 метров.

В основном, все электромагнитные обнаружители настроены на работу по данным параметрам. Временные параметры для поиска скрытых видеокамер при использовании электромагнитных приспособлений, зависят от того, какое количество камер уже есть в памяти такого приспособления. На сегодня, все электромагнитные приборы для обнаружения камер имеют индикацию света, звука и вибрации. А поиск скрытых видеокамер происходит практически незаметно для остальных людей. Максимально скрыто происходит поиск при помощи приспособлений, имеющих скрытую антенну. Но, если проводить обнаружение, когда такая антенна прилегает к человеческому телу, результат будет достигнут очень медленно, так как чувствительность антенны будет ниже. Чтобы достичь максимального эффекта, необходимо проводить процесс обнаружения, когда прибор находится на вытянутой руке и вокруг открытое пространство. Есть такие модели обнаружителей, в которых есть функция постоянного мониторинга пространства, а если обнаружен подозрительный сигнал, то он перенаправляется на удаленную ПЭВМ, возможен также обмен информации с персонального компьютера, используя обычный mini USB-порт, с его помощью можно обновлять данные или программное обеспечение. Электромагнитные определители намного чаще используются, чем оптические. Это связано с тем, что в последних не предусмотрена возможность вести скрытое обнаружение. Если человек анализирует помещение при помощи оптического приспособления, его точно заметят, а процесс обнаружения, чаще всего, должен оставаться в тайне для окружающих. Такие приспособления, помимо всего прочего, требуют больших затрат времени и предельной внимательности со стороны человека, который проводит процесс обнаружения. Но положительные качества у оптических приспособлений также присутствуют. В отличие от электромагнитных или радиоволновых, они могут зафиксировать все видеокамеры, даже те, которые на момент анализа помещения находятся выключенными. Когда стоит вопрос в выборе типа обнаружителя, следует обратить внимание на то, в какой ситуации будет происходить процесс обнаружения скрытых видеокамер. Если время выполнения поиска и скрытность не столь важны, то можно приобрести и оптический обнаружитель, который по цене в несколько раз дешевле, чем электромагнитный. Стоит так же

обратить внимание на универсальные обнаружители, которые совмещают в себе сразу несколько технологий обнаружения, но такие устройства и стоят в разы дороже.

Уникальные особенности "Antibug Hunter"

Прибор совмещает в себе сразу два устройства. Обнаружитель скрытых камер и детектор поля. Уникально! Теперь Вам нет необходимости тратить деньги на множество различных приборов. Вам достаточно приобрести один универсальный прибор "Antibug Hunter".

1.С его помощью Вы сможете произвести поиск скрытых и закамуфлированных камер, а также найти все радиопередающие устройства (жучки). Охватывает весь возможный диапазон, на которых работают жучки, от 1 до 6500 МГц.

2. Только "Antibug Hunter" имеет расширенный частотный диапазон, что позволяет Вам найти жучки, работающие на высоких частотах, которые не обнаруживаются другими приборами.

3. Возможность подключения наушников, для скрытого предупреждения при поиске закладных устройств. Применяя наушники при поиске жучков, становится возможным тайно контролировать ситуацию. Нет ли вблизи активных жучков. При выявлении жучка "Antibug Hunter" оповестит об этом тайно, звуковым сигналом через наушник и световой индикацией. Также имеется возможность настроить способ оповещения одновременно и светом и звуком (без наушников), в случае, где не требуется скрытый контроль. Например, необходимо проверить какое-либо помещение или автомобиль на наличие жучков.

4. Возможность скрытого предупреждения вибросигналом при поиске закладных устройств. В режиме обнаружения жучков прибор можно настроить на работу только со световой и вибро индикацией. Чем ближе прибор находится к источнику излучения, тем выше уровень светового сигнала на шкале и включается вибросигнал. Имеется возможность отрегулировать уровень чувствительности детектора в случае помех от расположенных неподалеку посторонних источников сигнала.

5. Три частоты мерцания светодиодов в режиме поиска камер. В режиме поиска камер прибор имеется возможность изменения частоты мерцания излучающих светодиодов. Это позволяет отсеять посторонние блики, мешающие понять где же на самом деле камера. Наиболее точно определить местоположение камеры поможет именно эта функция.

6. Другие преимущества прибора.

Компактные размеры 65х48х15 мм и легкий вес всего 40 гр. делают этот прибор портативным и удобным в использовании.

Настройка чувствительности позволяет адаптировать прибор к радиочастотному фону любого помещения.

Индикатор заряда аккумуляторной батареи.

Индикация разряда аккумуляторной батареи.

Возможность подключения наушников. Дополнительная внешняя антенна.

Методы обнаружения скрытых камер

Если раньше различные шпионские штучки в виде скрытых камер и прослушивающих жучков было практически невозможно достать, да и стоили они целое состояние и были доступны только спецслужбам и службам безопасности крупных компаний, то сегодня интернет пестрит предложениями по продаже этих приборов по вполне доступным ценам. Спрос на устройства скрытого видеонаблюдения также нешуточный, и купить такую камеру сегодня может любой желающий, поэтому если вы придерживаетесь мыслей «да кто будет за мной следить, кому я нужен?», то можете глубоко ошибаться. Сегодня скрытые камеры дешевы, доступны и могут использоваться в самых различных целях, даже людьми из вашего круга знакомств, которых вы совершенно не будете подозревать. Содержание: Как обнаружить скрытую камеру?

1. Визуальный метод Где и как искать?

2. Технический метод Вариации желающих «подсмотреть» за вами могут быть различными – арендодатели квартиры, которую вы снимаете, «бывшие», которые всячески хотят вам насолить, а также различные криминальные личности, желающие обнести вашу собственность. А если вас постоянно одолевает чувство, что за вами кто-то следит, почему бы не проверить ваши догадки практическим способом? Как обнаружить скрытую мини камеру? Как только в продажу выходит новое шпионское оборудование, находятся умельцы, которые тут же принимаются за разработку средств его обнаружения. Для обнаружения скрытых камер видеонаблюдения сегодня существуют специальные детекторы скрытых камер. Но для начала неплохо было бы просто провести тщательный визуальный осмотр помещения.

1. Визуальный метод

Скрытая камера под вещами Если у вас появилось подозрение, что за вами кто-то следит, то вы уже наверняка подозреваете и того, кто это может делать. Если это кто-то из вашего окружения (арендодатели, «бывшие», друзья), то в этом случае используемая техника будет довольно проста, и обнаружить скрытую камеру не составит большого труда даже при визуальном пристальном осмотре окружающего пространства. Если это правоохранительные органы или конкуренты, то можно говорить уже о более серьезной технике и профессиональной установке, и в таком случае обнаружить камеры будет уже не так-то просто. Также при поиске скрытой камеры необходимо представить, что именно хотел увидеть ее установщик – это значительно упростит поиск и сделает его более осмысленным. Где и как искать? Особое внимание следует уделить самым распространенным местам установки: Розеткам; Лампам; Люстрам; Комнатным растениям; Отверстиям шахт вентиляции; Различным щелям в стенах; Настенным и настольным часам и другим предметам, в которые легко можно встроить устройство скрытого наблюдения. Необходимо осмотреть все предметы домашнего обихода, даже те, которые вы бы ни за что не стали проверять на предмет наличия скрытых камер: Мягкие игрушки; Книги; Зеркала; Стекла; Коробки и другие предметы интерьера; Тщательно осмотрите углы комнаты. Когда скрытая камера устанавливается профессионалом, то найти вам ее вряд ли удастся, т. к. хорошо замаскированную миниатюрную беспроводную камеру обнаружить достаточно сложно. В таком случае необходимо обратиться в агентство по поиску шпионских устройств, или воспользоваться специальным детектором. К услугам агентства рекомендуется прибегать всем известным личностям, особенно тем, у кого есть домохозяйки и другой домашний персонал, посредством которых злоумышленники могут запросто расставить скрытые камеры. В таких агентствах, как правило, работают люди, прошедшие обучение в ФСБ. Стоимость услуг довольно приличная, и в среднем составляет 20$ за кв. метр, и зависит от сложности поиска и профессионализма специалиста, а если еще помещение завалено различного рода электроникой, то цена возрастает в разы. Еще один момент, который необходимо учитывать – специалисты ничего у вас не найдут, если слежка ведется правоохранительными органами, ибо не положено. Что же можно еще предпринять для самостоятельного обнаружения скрытой техники видеонаблюдения? Для начала стоит разобраться, по какому принципу функционируют камеры. Если это автономные устройства, то всю информацию они передают по беспроводным каналам: Wi-Fi; Радиоканалу; Посредством сети GSM или 3G; Или же записывают на внутренний накопитель. В случае записи на SD карту, человек, поставивший камеру, должен время от времени иметь доступ к устройству для снятия видеозаписей, и в этом случае его можно поймать за руку. При установке беспроводных мини видеокамер для обнаружения устройства можно использовать детекторы поля, подобные тем, которые применяются для поиска различных жучков. В случае, когда камера имеет встроенный источник питания, то наблюдатель также должен иметь к ней доступ для подзарядки устройства. Время автономной работы обычно не превышает 12 часов при установке записи по срабатыванию детектора движения.

2. Технический метод

В других случаях без применения специальной техники не обойтись. Практически любую скрытую камеру можно обнаружить в домашних условиях при помощи приборов, улавливающих блики оптики, подобно тому, как на фотографиях проявляется эффект красных глаз. Эти устройства называются видоискателями, они имеют подсветку и специальный светофильтр, глядя в который гораздо проще распознать отраженный свет от линзы объектива. Видоискатели камер. В большинстве случаев видоискатели имеют красную подсветку и красный светофильтр, благодаря которому влияние посторонних бликов существенно снижается. Подсветка подобных устройств может работать в импульсном режиме – яркая мигающая точка глазка объектива привлечет внимания явно больше, чем простая светящаяся. Стоимость простых видоискателей сегодня начинается от 2000 – 3000 р. в российских интернет магазинах. Чтобы найти скрытую камеру при помощи такого устройства необходимо включить подсветку и глядя в светофильтр осмотреть все самые рискованные места:

Углы между потолком и стенами;

Всю электронику;

Часы;

Предметы интерьера;

Головки болтов и саморезов на мебели, стенах, различных бытовых предметах – камера может быть спрятана где угодно.

При этом важно держать прибор как можно ближе к глазу, чтобы направление лучей подсветки совпадало с направлением взгляда – только так вы сможете увидеть свет, возвращаемый линзой объектива. Впрочем, все современные видоискатели скрытых камер построены таким образом, чтобы их было удобно держать около глаза – все они имеют миниатюрную форму, а светофильтр, в который нужно смотреть, располагается непосредственно в корпусе рядом со светодиодами.

Подобными характеристиками обладает простое устройство для обнаружения скрытых камер CC308+. Детектор имеет небольшие размеры и легко умещается в карман. В корпус прибора встроено шесть красных светодиодов и красный светофильтр. Также он имеет индикатор поля, и способен улавливать и беспроводную связь – GSM, Wi-Fi, радиосигнал, поэтому его применение не ограничено обнаружением скрытых камер – данное устройство можно вполне успешно использовать для поиска жучков прослушки. Устройство для обнаружения скрытых камер и жучков CC308plus Индикатор поля. Для поиска беспроводных камер, использующих связь по радиоканалу, рекомендуется применять так называемый индикатор поля (видеохантер), улавливающий сигнал передаваемый радиопередатчиком камеры. Данный прибор начинает вибрировать и пищать при появлении радиосигнала в зоне его нахождения. Индикатор поля + видоискатель Индикатор поля сегодня можно приобрести по вполне доступной цене, а размеры позволяют легко уместить прибор в кармане. Но есть у данного устройства неприятная особенность – большое количество ложных срабатываний, т. к. сегодня практически все окутано невидимой сетью различных беспроводных сетей, особенно в городской черте.

Видеохантер при обнаружении радиосигнала камеры перехватывает его и выводит изображение на экран, после чего обнаружить устройство скрытого видеонаблюдения не составит большого труда. Более профессиональное оборудование. Если этих приборов вам будет недостаточно, и вы решите провести доскональный осмотр помещения и окончательно развеять сомнения либо все-таки обнаружить тщательно замаскированную скрытую камеру, то вам необходимо более дорогостоящее оборудование:

Анализатор спектра;

Нелинейный локатор. Воспользоваться данными устройствами «с наскоку» у вас вряд ли получится – для их успешного использования необходимо иметь специальную подготовку. При помощи анализатора спектра можно выявить любой, даже зашифрованный радиосигнал, а нелинейный локатор обнаружит все электронные устройства, в которых используются осцилляторы. Если после поиска беспокойство относительно установки скрытых камер у вас осталось, в независимости от его результатов необходимо ограничить доступ посторонних лиц в помещение, а также регулярно проводить его тщательный осмотр на предмет подозрительных или «неправильно лежащих» предметов, которые могут сигнализировать о том, что здесь кто-то побывал без вашего ведома

3.Практическая работа на обнаружителе видеокамер.

Лабораторная работа 1

Обнаружение приборов наблюдения и оптических приборов

Цель работы: 1. Ознакомление студентов с работой аппаратуры определения оптических приборов и видеокамер.

2. Краткие теоретические сведения по принципам обнаружения.

3.Практическая работа на обнаружителе видеокамер.

Принцип обнаружения оптических приборов

Как правило, все подготовительные разведывательные действия террористического характера выполняются с применением разнообразных систем наблюдения (оптико-механических, телевизионных, ночного видения и прочих).

Одним из немногих демаскирующих признаков применения террористами и преступниками оптических приборов наблюдения, прицеливания и видения является их оптический контраст.

Активное применение обнаружителей оптических устройств дает возможность упредить действия террористов и преступников, которые могут привести к серьезным человеческим и материальным потерям и, кроме того, позволяет выиграть время для обеспечения реальной безопасности. Дальность обнаружения современных обнаружителей оптических устройств варьируется от 100 до 2500м.

Обнаружение оптических прицельно-наблюдательных приспособлений обеспечивается за счет эффекта световозвращения или «обратного блика». Этот эффект возникает, когда оптическое устройство освещается узконаправленным пучком света по оси оптического устройства или близко к ней и показан на рис. 2.

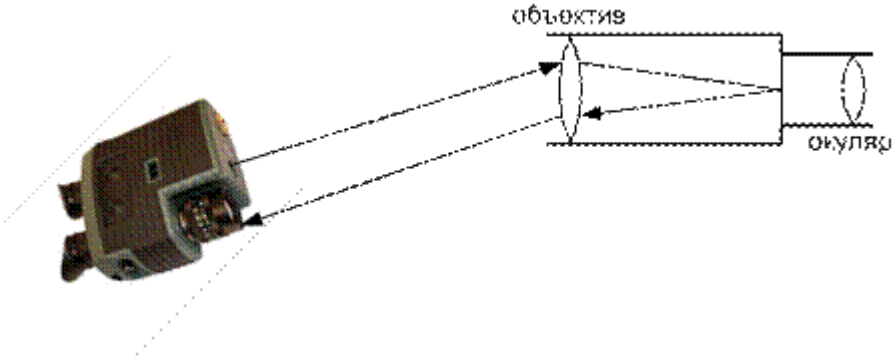


Рис. 2. Принцип действия обнаружителя оптических устройств

Яркость отраженного (световозвращающего) луча, как правило, на несколько порядков выше яркости диффузных вторичных источников, то есть непосредственно объектов, техники и местных предметов. Эффект будет возникать независимо от конструкции прицела и от того, что находится за ним. Свойства приборов позволяют обнаруживать оптическое и кино-фотонаблюдение, даже если оно ведется из-за тонированных или зеркальных стекол.

В зависимости от решаемой тактической задачи системы обнаружения оптических устройств делятся на стационарные и мобильные, портативные.

При установке систем на стационарных объектах предусмотрена организация работы как непосредственно с участием оператора, так и в автоматизированном режиме, с возможностью организации управления одновременно несколькими комплексами, с накоплением и передачей получаемой информации на удаленные пункты контроля.

Учитывая отсутствие у стационарных комплексов внешних отличий от стандартных охранно-телевизионных комплексов, исключается их ранняя идентификация со стороны террористов, ведущих наблюдение за объектом.

Мобильные и ручные приборы могут быть использованы в качестве эффективных средств предупреждения нападения, как на стационарные объекты, так и при организации надежной личной охраны руководителей и безопасности особо важных городских и загородных мероприятий.

В большинстве случаев обнаружители оптических устройств оснащаются инфракрасными лазерными излучателями и устройством наблюдения блика. Лазерные излучатели могут быть непрерывного и импульсного действия.

В приборах первого типа мощный лазер непрерывного действия, совмещенный с прибором ночного видения. Импульсные устройства совмещаются с инфракрасной видеокамерой и сложной логикой обработки сигнала, уменьшающей вероятность ложного обнаружения. Инфракрасная лазерная

подсветка используется, в основном, с целью предотвращения обнаружения снайпером средств обнаружения оптических устройств.

Для эффективного поиска оптических устройств, работающих в видимом диапазоне, длина волны лазера должна быть максимально приближена к длине волны оптического диапазона, так как коэффициенты преломления волн различной длины в оптических приборах также различны. Поэтому используется лазер с длиной волны 700..900 нм. Такое концентрированное излучение очень слабо воспринимается глазом.

Примером обнаружителей оптических устройств является устройство «СПИН-2» (рис. 3.), предназначенное для дистанционного обнаружения оптических и оптико-электронных средств, прицелов, длиннофокусных объективов в условиях как интенсивного дневного, так и слабого ночного освещения на расстоянии до 1000 м. Прибор позволяет регистрировать оптико-электронные средства наблюдения в виде яркого блика на фоне подстилающей поверхности. Угол пеленга средств наблюдения соответствует углу поля зрения самих средств наблюдения. Визуализация наблюдаемых объектов осуществляется через встроенный электронный псевдобинокуляр.

Рис. 3. Средство обнаружения оптических устройств «СПИН-2»

Существуют портативные устройства, предназначенные для поиска скрытно установленных видео-фото-камер и других скрытых оптических устройств. Работают такие устройства по такому же принципу, однако имеются конструктивные отличия. Они обнаруживают оптику любого типа, даже если фотоаппарат или камера выключены, работают на расстояниях 5…20 м, что вполне достаточно, для того, чтобы обнаружить скрытно установленное в помещении оптическое устройство. В них используется видимый оптический диапазон, делая невозможным применение различного рода фильтров, т.к. фильтр сделает невозможным наблюдение скрытно установленным устройством.

Примером данного класса устройств является обнаружитель скрытых видеокамер «ВОРОН» (рис. 4), предназначен для быстрого обнаружения и определения местоположения скрытых (камуфлированных в различные предметы интерьера и одежды) микровидеокамер, в том числе с объективами типа «Pin-hole». Обнаружитель «ВОРОН» использует светодиодную подсветку целей, что гарантирует безопасность эксплуатации и отсутствие вредного воздействия на человека (в отличие от лазерной подсветки). Дальность обнаружения объективов скрытых видеокамер типа Pin-Hole (ø 1 мм) составляет от 1 до 20 метров.

Средства обнаружения скрытых видеокамер

Сегодня технологии развиты до такой степени, что как только появляется новое приспособление для прослушки или скрытого видеонаблюдения, так тут же создаются средства, способные обнаружить и нейтрализовать такое приспособление. Устройства, позволяющие обеспечить безопасность какому-либо объекту, постоянно усовершенствуются, в них появляются новые функции и возможности для более эффективного использования. Точно так же происходит совершенствование устройств для обнаружения скрытых видеокамер. Многие злоумышленники потратили немало времени и сил для создания приборов скрытой фото- и видеосъемки, а также способов ночного наблюдения. Каждый раз создавалась видеокамера меньшего размера, чем ее предшественница, но с лучшими техническими характеристиками, благодаря которым улучшалось качество изображения. В зависимости от поставленных перед шпионом целей, выделяют видеокамеры проводные и беспроводные, работающие дистанционно или передающие изображение по радиоканалу. На сегодняшний момент, злоумышленник может установить камеру где угодно за считанные секунды - на одежде, на мебели, на стенах и так далее, а съемка будет проходить незаметно ни для кого. Пока известно три метода, применяя которые можно засечь скрытые камеры видеонаблюдения:

Применяется индикатор поля. Этот вариант подходит в том случае, когда информация передается по радиоканалу.

Применение оптических приспособлений. В этом случае лазерный луч прибора отражается от объектива скрытой видеокамеры.

Использование электромагнитного обнаружителя скрытых камер видеонаблюдения.

Радиолокация

Приборы, с помощью которых проводится поиск скрытых видеокамер, согласно первого способа являются самым обыкновенным индикатором поля. Такие приспособления очень часто используются на Западе. Они определяют все устройства, которые работают по радиоканалу и даёт возможность их заблокировать. Подобные технические средства, соответственно, позволяют обнаружить лишь беспроводные камеры, а так же другие типы жучков, использующих радиоканал для передачи данных.

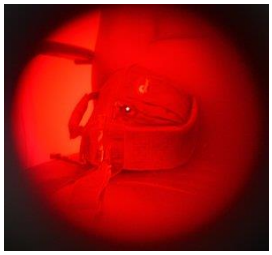
Оптическое исследование

Оптические приборы настроены на функционирование по принципу световозвращения. Объяснить это можно тем, что все приспособления для наблюдения и скрытые видеокамеры в том числе, оснащены ПЗС-матрицей или другим элементом обладающим светочувствительным свойством и если на него направить лазерный луч, он отразится обратно к обнаружителю. Поэтому, для определения скрытой камеры достаточно направить лазерный луч прибора оптического типа на то место, где возможно размещена камера и будет заметен блик от светоотражающего элемента. Современные оптические приборы усовершенствованы до такой степени, что могут отсеивать излучения, исходящие от других приборов кроме камер. Для этих целей в устройства часто устанавливают ИК-пропускающий фильтр и четко подбирают

параметры для лазерного луча.

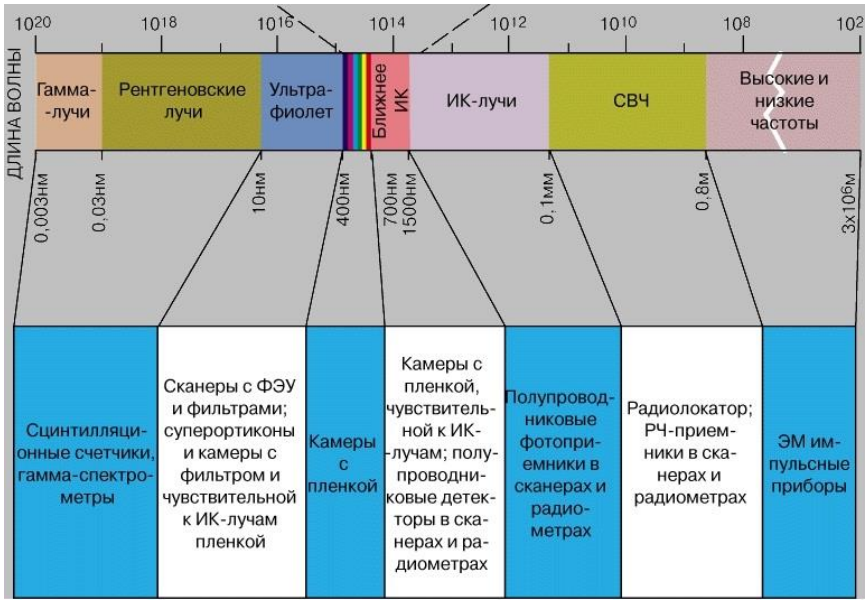
Оптический способ для обнаружения скрытых камер имеет как преимущества, так и недостатки. Таким способом можно легко засечь любое оптическое приспособление, будь то бинокль или снайперская

винтовка. Однако, сегодня разработано множество светофильтров, способных отсеивать световые волны определенной длины.



Анализ электромагнитного поля

Третий способ, который позволяет зафиксировать скрытые камеры видеонаблюдения – это использование электромагнитных приспособлений (обнаружителей). Чтоб понять как они работают,необходимо знать из чего состоят сами камеры. В основной массе видеокамер установлена ПЗС-матрица в роли фотоприемника (приспособление, способное трансформировать световой сигнал в электрический). Такая матрица функционирует благодаря считывателю сигнала, то есть процессору, который впоследствии и создает сам видеосигнал. В процессоре есть осциллятор, он образует излучение на указанной частоте. Осциллятор способен излучать энергию лишь на маленькие расстояние, но имеет и другие излучения, которые состоят из гармоник главной частоты. Среди этих гармоник есть такие, которые способны очень хорошо проходить через корпус видеокамеры. Есть такой тип камер, который производит очень большое излучение на гармониках, а изображение записывается в память обнаружителя. Для каждой разновидности камер может быть свойственное только определённое излучение, поэтому обнаружитель содержит в памяти основные волновые характеристики большинства видеокамер, чтобы отсеивать волны, поступающие от сторонних электроприборов.



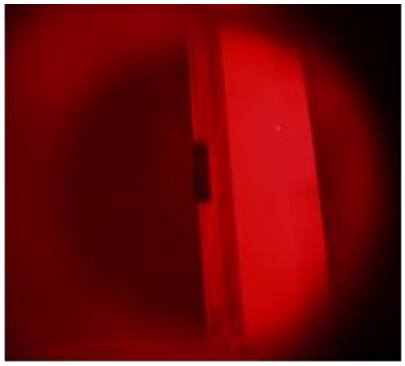
Как же происходит процесс обнаружения камер? Приспособление проводит анализ электромагнитных частот, которые находятся в периметре, и проводит сравнение с теми, которые заранее находятся в его памяти. Обнаружитель во время всего процесса делит полосу спектра, в котором находится осциллятор камеры, на небольшие сегменты, медленно повышая чувствительность. После чего обнаружитель определяет, что это за частота - скрытой камеры наблюдения или просто посторонняя помеха. Чтобы отсечь такого рода помехи, часто используют двойную верификацию и подтверждение. Встречаются участки, которые требуют тщательного анализа, бывает, проверка происходит четыре раза и только тогда удается определить, что за излучение - частота случайных помех или осциллятора скрытой камеры.

Особенности обнаружителей

Сегодня на рынке представлен широкий ассортимент видеокамер, самых разнообразных типов, обладающих несходными друг с другом техническими характеристиками. На территории России чаще всего используют видеокамеры PAL, на втором месте стоит камера типа NTSC, все остальные очень редко встречаются на практике. Систематизация образов в память камеры у всех разновидностей камер отличается. Есть камеры, в которых предусмотрена функция фиксирования образов, что находятся во

встроенной памяти видеокамеры. А во многих других камерах эти образы сбрасываются. Частота осциллятора меняется от температуры воздуха в помещении и от электронных составляющих самого приспособления. Злоумышленники часто используют камеры дистанционного управления, в этом случае, после ее включения она прогревается и в обнаруженном ранее спектре ее уже не выявить. То есть через некий промежуток времени камера просто исчезает, и время на ее обнаружение было зря потеряно. Когда происходит процесс обнаружения скрытой камеры наблюдения, то на экране обнаружителя видеокамер показывается, какой уровень излучения исходит от анализированного участка, одни приборы настроены на отображение интегрального уровня излучения, а некоторые другие - отображают на дисплее наибольшую гармонику.

Видеокамера в галстуке



Видеокамера в стене лестничной площадки

Видеокамера в копировальном аппарате

Большего результата позволяет достичь использование второго варианта, так как в интегральном уровне может исчезнуть одна гармоника, попасть в зону, где ее невозможно зафиксировать. Это объясняется тем, что благодаря интерференции наложения волн их отражения значительно увеличиваются, а иногда и вовсе пропадают, из-за этого интегральный уровень полностью изменяется, по этой причине может произойти обнаружение скрытой видеокамеры в том участке, где ее и вовсе нет. И оптические приспособления, и электромагнитные способны зафиксировать наличие камеры в промежутке нескольких метров.

Оптический обнаружитель всех видов скрытых камер "Филин" предназначен для поиска спрятанных камер видео наблюдения. С помощью этого устройства Вы сможете без труда найти любые камеры вне зависимости от их состояния, включены они или выключены. Это могут быть проводные или беспроводные, скрытые или закамуфлированные.

Обнаружитель камер "Беркут", предназначен для поиска скрытых (закамуфлированных в различные предметы интерьера) видеокамер в не зависимости от их состояния. Находятся они во включенном или в выключенном состоянии. Обнаружитель скрытых видеокамер "Беркут" позволяет выявить как проводные камеры, так и видеокамеры, работающие по радиоканалу (беспроводные).

Дальность обнаружения

Дальность обнаружения оптических приборов зависит от того, какой тип подсветки установлен - непрерывная или импульсная; от возможности настройки по диоптриям; от того, какое зрение у человека, который проводит анализ помещения; от уровня освещения в исследуемом помещении и от многих других факторов.

При использовании электромагнитных обнаружителей, на дальность функционирования приспособления влияют тип камеры и то, каким образом от нее происходит излучение.

Если камера очень слабо излучает, то ее можно зафиксировать на расстоянии около трех метров.

Те камеры, которые настроены на высокое излучение, обнаруживаются в пределах 50 метров. Среднее излучение можно засечь в диапазоне 7-10 метров.

В основном, все электромагнитные обнаружители настроены на работу по данным параметрам. Временные параметры для поиска скрытых видеокамер при использовании электромагнитных приспособлений, зависят от того, какое количество камер уже есть в памяти такого приспособления. На сегодня, все электромагнитные приборы для обнаружения камер имеют индикацию света, звука и вибрации. А поиск скрытых видеокамер происходит практически незаметно для остальных людей. Максимально скрыто происходит поиск при помощи приспособлений, имеющих скрытую антенну. Но, если проводить обнаружение, когда такая антенна прилегает к человеческому телу, результат будет достигнут очень медленно, так как чувствительность антенны будет ниже. Чтобы достичь максимального эффекта, необходимо проводить процесс обнаружения, когда прибор находится на вытянутой руке и вокруг открытое пространство. Есть такие модели обнаружителей, в которых есть функция постоянного мониторинга пространства, а если обнаружен подозрительный сигнал, то он перенаправляется на удаленную ПЭВМ, возможен также обмен информации с персонального компьютера, используя обычный mini USB-порт, с его помощью можно обновлять данные или программное обеспечение. Электромагнитные определители намного чаще используются, чем оптические. Это связано с тем, что в последних не предусмотрена возможность вести скрытое обнаружение. Если человек анализирует помещение при помощи оптического приспособления, его точно заметят, а процесс обнаружения, чаще всего, должен оставаться в тайне для окружающих. Такие приспособления, помимо всего прочего, требуют больших затрат времени и предельной внимательности со стороны человека, который проводит процесс обнаружения. Но положительные качества у оптических приспособлений также присутствуют. В отличие от электромагнитных или радиоволновых, они могут зафиксировать все видеокамеры, даже те, которые на момент анализа помещения находятся выключенными. Когда стоит вопрос в выборе типа обнаружителя, следует обратить внимание на то, в какой ситуации будет происходить процесс обнаружения скрытых видеокамер. Если время выполнения поиска и скрытность не столь важны, то можно приобрести и оптический обнаружитель, который по цене в несколько раз дешевле, чем электромагнитный. Стоит так же обратить внимание на универсальные обнаружители, которые совмещают в себе сразу несколько технологий обнаружения, но такие устройства и стоят в разы дороже.

Уникальные особенности "Antibug Hunter"

Прибор совмещает в себе сразу два устройства. Обнаружитель скрытых камер и детектор поля. Уникально! Теперь Вам нет необходимости тратить деньги на множество различных приборов. Вам достаточно приобрести один универсальный прибор "Antibug Hunter".

1.С его помощью Вы сможете произвести поиск скрытых и закамуфлированных камер, а также найти все радиопередающие устройства (жучки). Охватывает весь возможный диапазон, на которых работают жучки, от 1 до 6500 МГц.

2. Только "Antibug Hunter" имеет расширенный частотный диапазон, что позволяет Вам найти жучки, работающие на высоких частотах, которые не обнаруживаются другими приборами.

3. Возможность подключения наушников, для скрытого предупреждения при поиске закладных устройств. Применяя наушники при поиске жучков, становится возможным тайно контролировать ситуацию. Нет ли вблизи активных жучков. При выявлении жучка "Antibug Hunter" оповестит об этом тайно, звуковым

сигналом через наушник и световой индикацией. Также имеется возможность настроить способ оповещения одновременно и светом и звуком (без наушников), в случае, где не требуется скрытый контроль. Например, необходимо проверить какое-либо помещение или автомобиль на наличие жучков.

4. Возможность скрытого предупреждения вибросигналом при поиске закладных устройств. В режиме обнаружения жучков прибор можно настроить на работу только со световой и вибро индикацией. Чем ближе прибор находится к источнику излучения, тем выше уровень светового сигнала на шкале и включается вибросигнал. Имеется возможность отрегулировать уровень чувствительности детектора в случае помех от расположенных неподалеку посторонних источников сигнала.

5. Три частоты мерцания светодиодов в режиме поиска камер. В режиме поиска камер прибор имеется возможность изменения частоты мерцания излучающих светодиодов. Это позволяет отсеять посторонние блики, мешающие понять где же на самом деле камера. Наиболее точно определить местоположение камеры поможет именно эта функция.

6. Другие преимущества прибора.

Компактные размеры 65х48х15 мм и легкий вес всего 40 гр. делают этот прибор портативным и удобным в использовании.

Настройка чувствительности позволяет адаптировать прибор к радиочастотному фону любого помещения.

Индикатор заряда аккумуляторной батареи.

Индикация разряда аккумуляторной батареи.

Возможность подключения наушников. Дополнительная внешняя антенна.

Методы обнаружения скрытых камер

Если раньше различные шпионские штучки в виде скрытых камер и прослушивающих жучков было практически невозможно достать, да и стоили они целое состояние и были доступны только спецслужбам и службам безопасности крупных компаний, то сегодня интернет пестрит предложениями по продаже этих приборов по вполне доступным ценам. Спрос на устройства скрытого видеонаблюдения также нешуточный, и купить такую камеру сегодня может любой желающий, поэтому если вы придерживаетесь мыслей «да кто будет за мной следить, кому я нужен?», то можете глубоко ошибаться. Сегодня скрытые камеры дешевы, доступны и могут использоваться в самых различных целях, даже людьми из вашего круга знакомств, которых вы совершенно не будете подозревать. Содержание: Как обнаружить скрытую камеру?

1. Визуальный метод Где и как искать?

2. Технический метод Вариации желающих «подсмотреть» за вами могут быть различными – арендодатели квартиры, которую вы снимаете, «бывшие», которые всячески хотят вам насолить, а также различные криминальные личности, желающие обнести вашу собственность. А если вас постоянно одолевает чувство, что за вами кто-то следит, почему бы не проверить ваши догадки практическим способом? Как обнаружить скрытую мини камеру? Как только в продажу выходит новое шпионское оборудование, находятся умельцы, которые тут же принимаются за разработку средств его обнаружения. Для обнаружения скрытых камер видеонаблюдения сегодня существуют специальные детекторы скрытых камер. Но для начала неплохо было бы просто провести тщательный визуальный осмотр помещения.

1. Визуальный метод

Скрытая камера под вещами Если у вас появилось подозрение, что за вами кто-то следит, то вы уже наверняка подозреваете и того, кто это может делать. Если это кто-то из вашего окружения (арендодатели, «бывшие», друзья), то в этом случае используемая техника будет довольно проста, и обнаружить скрытую камеру не составит большого труда даже при визуальном пристальном осмотре окружающего пространства. Если это правоохранительные органы или конкуренты, то можно говорить уже о более серьезной технике и профессиональной установке, и в таком случае обнаружить камеры будет уже не так-то просто. Также при поиске скрытой камеры необходимо представить, что именно хотел увидеть ее установщик – это значительно упростит поиск и сделает его более осмысленным. Где и как искать? Особое внимание следует уделить самым распространенным местам установки: Розеткам; Лампам; Люстрам; Комнатным растениям; Отверстиям шахт вентиляции; Различным щелям в стенах; Настенным и настольным часам и другим предметам, в которые легко можно встроить устройство скрытого наблюдения. Необходимо осмотреть все предметы домашнего обихода, даже те, которые вы бы ни за что не стали проверять на предмет наличия

скрытых камер: Мягкие игрушки; Книги; Зеркала; Стекла; Коробки и другие предметы интерьера; Тщательно осмотрите углы комнаты. Когда скрытая камера устанавливается профессионалом, то найти вам ее вряд ли удастся, т. к. хорошо замаскированную миниатюрную беспроводную камеру обнаружить достаточно сложно. В таком случае необходимо обратиться в агентство по поиску шпионских устройств, или воспользоваться специальным детектором. К услугам агентства рекомендуется прибегать всем известным личностям, особенно тем, у кого есть домохозяйки и другой домашний персонал, посредством которых злоумышленники могут запросто расставить скрытые камеры. В таких агентствах, как правило, работают люди, прошедшие обучение в ФСБ. Стоимость услуг довольно приличная, и в среднем составляет 20$ за кв. метр, и зависит от сложности поиска и профессионализма специалиста, а если еще помещение завалено различного рода электроникой, то цена возрастает в разы. Еще один момент, который необходимо учитывать – специалисты ничего у вас не найдут, если слежка ведется правоохранительными органами, ибо не положено. Что же можно еще предпринять для самостоятельного обнаружения скрытой техники видеонаблюдения? Для начала стоит разобраться, по какому принципу функционируют камеры. Если это автономные устройства, то всю информацию они передают по беспроводным каналам: Wi-Fi; Радиоканалу; Посредством сети GSM или 3G; Или же записывают на внутренний накопитель. В случае записи на SD карту, человек, поставивший камеру, должен время от времени иметь доступ к устройству для снятия видеозаписей, и в этом случае его можно поймать за руку. При установке беспроводных мини видеокамер для обнаружения устройства можно использовать детекторы поля, подобные тем, которые применяются для поиска различных жучков. В случае, когда камера имеет встроенный источник питания, то наблюдатель также должен иметь к ней доступ для подзарядки устройства. Время автономной работы обычно не превышает 12 часов при установке записи по срабатыванию детектора движения.

2. Технический метод

В других случаях без применения специальной техники не обойтись. Практически любую скрытую камеру можно обнаружить в домашних условиях при помощи приборов, улавливающих блики оптики, подобно тому, как на фотографиях проявляется эффект красных глаз. Эти устройства называются видоискателями, они имеют подсветку и специальный светофильтр, глядя в который гораздо проще распознать отраженный свет от линзы объектива. Видоискатели камер. В большинстве случаев видоискатели имеют красную подсветку и красный светофильтр, благодаря которому влияние посторонних бликов существенно снижается. Подсветка подобных устройств может работать в импульсном режиме – яркая мигающая точка глазка объектива привлечет внимания явно больше, чем простая светящаяся. Стоимость простых видоискателей сегодня начинается от 2000 – 3000 р. в российских интернет магазинах. Чтобы найти скрытую камеру при помощи такого устройства необходимо включить подсветку и глядя в светофильтр осмотреть все самые рискованные места:

Углы между потолком и стенами;

Всю электронику;

Часы;

Предметы интерьера;

Головки болтов и саморезов на мебели, стенах, различных бытовых предметах – камера может быть спрятана где угодно.

При этом важно держать прибор как можно ближе к глазу, чтобы направление лучей подсветки совпадало с направлением взгляда – только так вы сможете увидеть свет, возвращаемый линзой объектива. Впрочем, все современные видоискатели скрытых камер построены таким образом, чтобы их было удобно держать около глаза – все они имеют миниатюрную форму, а светофильтр, в который нужно смотреть, располагается непосредственно в корпусе рядом со светодиодами.

Подобными характеристиками обладает простое устройство для обнаружения скрытых камер CC308+. Детектор имеет небольшие размеры и легко умещается в карман. В корпус прибора встроено шесть красных светодиодов и красный светофильтр. Также он имеет индикатор поля, и способен улавливать и беспроводную связь – GSM, Wi-Fi, радиосигнал, поэтому его применение не ограничено обнаружением скрытых камер – данное устройство можно вполне успешно использовать для поиска жучков

прослушки. Устройство для обнаружения скрытых камер и жучков CC308plus Индикатор поля. Для поиска беспроводных камер, использующих связь по радиоканалу, рекомендуется применять так называемый индикатор поля (видеохантер), улавливающий сигнал передаваемый радиопередатчиком камеры. Данный прибор начинает вибрировать и пищать при появлении радиосигнала в зоне его нахождения. Индикатор поля + видоискатель Индикатор поля сегодня можно приобрести по вполне доступной цене, а размеры позволяют легко уместить прибор в кармане. Но есть у данного устройства неприятная особенность – большое количество ложных срабатываний, т. к. сегодня практически все окутано невидимой сетью различных беспроводных сетей, особенно в городской черте.

Видеохантер при обнаружении радиосигнала камеры перехватывает его и выводит изображение на экран, после чего обнаружить устройство скрытого видеонаблюдения не составит большого труда. Более профессиональное оборудование. Если этих приборов вам будет недостаточно, и вы решите провести доскональный осмотр помещения и окончательно развеять сомнения либо все-таки обнаружить тщательно замаскированную скрытую камеру, то вам необходимо более дорогостоящее оборудование:

Анализатор спектра;

Нелинейный локатор. Воспользоваться данными устройствами «с наскоку» у вас вряд ли получится – для их успешного использования необходимо иметь специальную подготовку. При помощи анализатора спектра можно выявить любой, даже зашифрованный радиосигнал, а нелинейный локатор обнаружит все электронные устройства, в которых используются осцилляторы. Если после поиска беспокойство относительно установки скрытых камер у вас осталось, в независимости от его результатов необходимо ограничить доступ посторонних лиц в помещение, а также регулярно проводить его тщательный осмотр на предмет подозрительных или «неправильно лежащих» предметов, которые могут сигнализировать о том, что здесь кто-то побывал без вашего ведома

3.Практическая работа на обнаружителе видеокамер.

Лабораторная работа 2-4.

Тема «Поиск каналов утечки информации с помощью нелинейного локатора. Поиск и обнаружение радиозакладок в помещении»

Место проведения : -класс 107

Цель работы: изучить методы противодействия несанкционированному съему информации с помощью радиозакладок, получить навыки практического использования данных методов.

Задача:

1. Изучить теоретический материал методики работы с нелинейными локаторами.
2. Получить задание на работу (см. Приложение).
3. Выполнить заданит по поискау закладного устройства.
4. Составить отчет (см. Приложение

ОБНАРУЖЕНИЕ ПОЛУПРОВОДНИКОВЫХ ЭЛЕМЕНТОВ
С ПОМОЩЬЮ НЕЛИНЕЙНОГО ЛОКАТОРА
1. ОСНОВНЫЕ ФИЗИЧЕСКИЕ ПРЕДПОСЫЛКИ

Основным фактором, препятствующим использованию радиолокационного метода для создания дистанционных средств поиска неподвижных малоразмерных объектов, является значительный уровень помех от окружающего фона. Практическое отсутствие нелинейных электромагнитных свойств у естественного фона (грунта, воды, растительности) позволяет регистрировать гармоники облучающего поля, возникающие за счет наличия объектов искусственного происхождения, находящихся в зоне поиска на поверхности грунта или в его верхнем слое. Нелинейными свойствами могут обладать некоторые горные породы с высокой концентрацией ферромагнитных включений, а также отдельные залежи сульфидных руд. Известно, что у

реальных объектов наибольшими нелинейными свойствами обладают высокочастотные полупроводниковые радиодетали (транзисторы, диоды), а также точечные прижимные стальные контакты.

Такими объектами являются (таблица 1): различные радиоуправляемые устройства и устройства промышленного шпионажа, стрелковое оружие, обломки самолетов и вертолетов, переносные радиостанции (в том числе и выключенные) и т.д. Объектами поиска могут быть также специальные нелинейные метки, используемые для скрытого обозначения различных объектов и участков местности, а также людей (например, спасателей в труднодоступных местах).

Таблица 1. Объекты поиска в нелинейной радиолокации

Объекты поиска		Нелинейные элементы объектов поиска	Области применения нелинейной локации (варианты)
Устройства промышленного шпионажа	аудио	П/п радиодетали модулятора и УКВ микропередатчика	«Чистка» помещений от Устройств коммерческой разведки конкурентов
	видео	Фотоприемники, п/п Радиодетали УВЧ (СВЧ) микропередатчика	
Радиоуправляемые устройства	П/п радиодетали схемы радиоприемника и блока управления состоянием объекта		Предотвращение террористических актов
Обломки самолетов и вертолетов	Точечные контакты отдельных металлических элементов и обломков между собой. Обломки радиоэлектронной аппаратуры		Дистанционное обнаружение обломков в труднодоступных местах (тайга, горы и т.д.)
Стрелковое оружие	Точечные и плоскостные металлические контакты деталей и патронов		Дистанционное обнаружение террористических групп с воздушных носителей
Переносные радиостанции и ЗРК	П/п радиодетали передатчика, приемника и системы наведения ЗРК		Дистанционное обнаружение террористических групп с воздушных носителей
Нелинейные маркеры	Полупроводниковые диоды, нагруженные на антенны-отражатели		Дистанционное маркирование подземных объектов, «черных ящиков» самолетов, участков местности и спасателей с земли и воздуха

Способность нелинейного локатора обнаруживать радиоэлектронные устройства основана на следующем. Любые радиоэлектронные устройства (РЭУ), независимо от размера и функционального назначения, состоят из печатных плат с проводниками, которые представляют для зондирующего сигнала локатора набор элементарных антенн - вибраторов. В разрыв отдельных проводников включены полупроводниковые элементы: диоды, транзисторы, микросхемы [53].

В результате облучения РЭУ зондирующим сигналом на частоте f на его полупроводниковых элементах через элементарные антенны наводится переменная ЭДС. В силу нелинейного характера вольт- амперной характеристики (ВАХ) элементов РЭУ переменный сигнал высокой частоты локатора претерпевает нелинейное преобразование в набор гармоник, частоты которых равны кратному целому числу зондирующей частоты локатора (2f, 3f и т.д.). С помощью тех же самых проводников печатной платы (элементарных антенн) весь спектр, включающий сигналы как на основной частоте f, так и на частотах гармоник 2f, 3f и т.д., переизлучается в эфир. Приемник локатора, принимая любую высшую гармонику переотраженного зондирующего сигнала локатора, устанавливает наличие в зоне облучения РЭУ [16, 53].

Так как амплитуда сигнала на гармонике резко убывает с увеличением ее номера, то в нелинейных локаторах в основном используют 2-ю и реже 3-ю гармоники.

Коэффициент преобразования энергии зондирующего сигнала в энергию высших гармоник очень мал, что относит нелинейные локаторы к системам ближнего действия. Существенное влияние на величину коэффициента преобразования оказывают значения мощности и частоты зондирующего сигнала локатора. Зависимость коэффициента преобразования от мощности зондирующего сигнала в первом приближении с точностью до 80% повторяет структуру ВАХ полупроводниковых элементов. Следовательно, на процесс преобразования влияет не величина средней мощности, а пиковая (импульсная) мощность сигнала [16, 53].

Сам процесс преобразования не зависит от состояния РЭУ: активное (включенное) или пассивное (выключенное), но коэффициент преобразования, а, следовательно, и мощность сигнала гармоник, являются функцией состояния объекта. При активном режиме объекта поиска мощность переизлученного на гармониках сигнала возрастает [53].

Наличие нелинейности характерно не только для полупроводниковых элементов радиоэлектронных средств, но контактов между металлическими предметами с пленкой окислов на поверхности, например, ржавых прутьев в железобетонных плитах домов. Все металлические контакты, в том числе и ржавчина, представляют собой нелинейный элемент с неустойчивым p-n переходом, поскольку он образован путем естественного прижима двух или более поверхностей. В физике полупроводников подобная структура известна как структура металл-окисел-металл, а нелинейный элемент подобной структуры называется МОМ-диод [53]. Поэтому обнаружение 2-й гармоники в отраженном сигнале не является достаточным условием наличия закладного устройства. Одновременный анализ 2-й и 3-й гармоник позволяет приближенно провести селекцию их источников: полупроводников РЭУ и других металлических элементов с полупроводниковым эффектом. Только в результате последующего обследования места облучения достоверно выявляется закладное устройство.

Как правило, на индикаторном устройстве современного нелинейного локатора отображаются относительные уровни принимаемых сигналов на второй и третьей гармониках и их разница. Индикаторные устройства располагаются или на приемо-передающем блоке (локаторы Super Broom, "Омега-3" и др.), или непосредственно на антенной штанге (локаторы NJE - 4000, NR-900E, "Энвис" и др.).

В нелинейных локаторах в основном используются передающие антенны с линейной поляризацией и приемные антенны - с круговой поляризацией.

Проникающая глубина зондирующего сигнала зависит от мощности и частоты излучения. Вследствие увеличения затухания электромагнитной волны в среде распространения с повышением частоты зондирующего сигнала (с ростом частоты наблюдается экспонен-циальный рост затухания) и вследствие физической природы процесса преобразования частоты полупроводниковыми приборами, связанной с их частотными свойствами, и в частности с граничной рабочей частотой, уровень мощности преобразованного отраженного сигнала тем выше, чем ниже частота зондирующего сигнала локатора [53]. Но для излучений с более низкой частотой ухудшаются возможности локатора по локализации места нахождения нелинейности, так как при приемлемых размерах его антенны расширяется ее диаграмма направленности. В основном в нелинейных локаторах используются частоты от 600 до 1 000 МГц [53].

При выборе частоты зондирующего сигнала необходимо учитывать и тот факт, что приемники нелинейных локаторов обладают высокой чувствительностью, поэтому на частотах приема не должно быть сигналов посторонних радиоэлектронных средств даже сравнительно небольшого уровня. В противном случае наличие мешающих сигналов значительно затрудняет процесс поиска закладных устройств. Например, в центре Москвы работа с нелинейным локатором "Энвис" может быть затруднена, так как в полосе приема отраженного сигнала на второй гармонике (около 1806 МГц) постоянно работает мощное радиоэлектронное средство.

Поэтому наиболее эффективно применение нелинейных локаторов, имеющих возможность перестройки рабочей частоты в некотором диапазоне. Например, в нелинейном локаторе Orion (NJE - 400) фирмы Research Electronics International (REI) предусмотрен автоматический режим выбора рабочей частота в диапазоне от 880 до 1000 МГц. При этом в качестве рабочей выбирается частота, на второй гармонике которой наблюдается наименьший уровень помех.

2. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ НЕЛИНЕЙНОЙ ЛОКАЦИИ

Антенна нелинейного локатора (НЛ) облучает объект для определения наличия в нем электронных компонентов. Когда ВЧ сигнал облучает полупроводниковые соединения (диоды, транзисторы и т.д.), он возвращается на гармонических частотах с определенными уровнями, благодаря нелинейным характеристикам соединения.

Однако ложные срабатывания также могут иметь при этом место, из-за того, что

места соединения двух различных металлов или коррозионные металлические конструкции также вызывают гармонический отраженный сигнал вследствие своих нелинейных характеристик. Такие соединения мы будем называть ложными.
На рис.1 представлены вольт-амперные характеристики полупроводникового и ложного соединений.

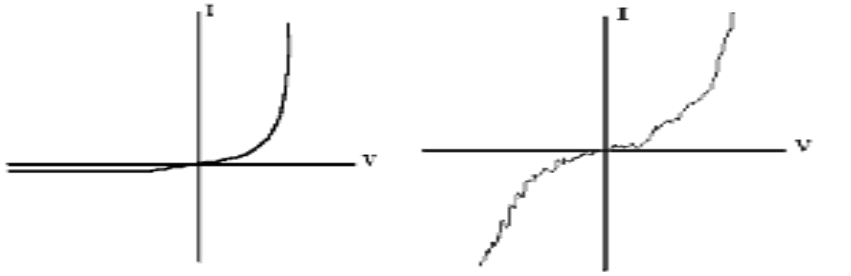


Рис.1. Вольт-амперные характеристики полупроводникового и ложного соединений
Из-за различия в нелинейных характеристиках полупроводникового и ложного соединений, отклики 2-й и 3-й гармоник будут иметь различную интенсивность. Когда НЛ облучает полупроводник, отклик на второй гармонике сильнее, чем на 3-ей. При облучении ложного соединения наблюдается обратный эффект: отклик на 3-ей гармонике сильнее, чем на 2-ой.

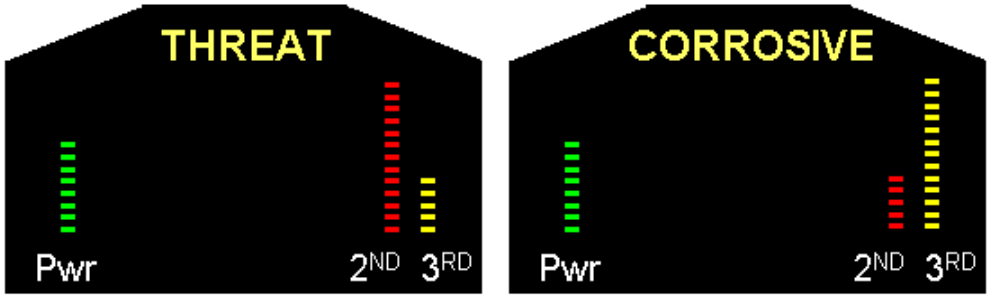


Рис.2. Сравнение уровней сигналов 2-ой и 3-ей гармоник при работе с НЛ
(слева - полупроводник, справа - ложное соединение)
На основе накопленных экспериментальных и физических представлений процесс наблюдения в условиях нелинейной локации полностью аналогичен традиционной локации для случая наблюдения объектов с активным ответом в режиме опознавания, при этом уравнение нелинейной радиолокации будет иметь вид

$$P_{N_{пр.}} = \frac{P_{изл.} G_{изл.} G_{N_{пр.}} \lambda^2}{(4\pi r)^4} \cdot \frac{\lambda^2}{N^2} \cdot G_{НО_{пр.}} G_{N_{изл.}} \xi_N(\omega, P_{изл.}) \cdot K_1(\omega) K_2(\omega_N), \quad (1)$$

где $P_{N_{пр.}}$ — мощность отклика объекта на N-й гармонике в месте расположения приёмной антенны локатора; $P_{изл.}$ — мощность излучения локатора; $G_{изл.}$ — коэффициент усиления излучающей антенны локатора; $G_{N_{пр.}}$ — коэффициент усиления приёмной антенны локатора на N-й гармонике; $\lambda = c/f$ — длина волны излучения локатора (эквивалентна частоте, где c — скорость света, f — частота излучения локатора); r — расстояние до объекта; N — номер принимаемой локатором гармоники; $G_{НО_{пр.}}$ — коэффициент усиления эквивалентной приёмной антенны нелинейного объекта; $G_{N_{изл.}}$ — коэффициент усиления эквивалентной излучающей антенны нелинейного объекта; $K_1(\omega)$ — частотно-зависимый коэффициент затухания зондирующего сигнала локатора в среде распространения; $K_2(\omega_N)$ — частотно-зависимый коэффициент затухания сигнала N-й гармоники от объекта в среде распространения; $\xi_N(\omega, P_{изл.})$ — коэффициент нелинейного преобразования для N-й гармоники, который, как будет показано ниже, зависит от частоты и мощности излучения локатора.

[1]: Анализ выражения (1) показывает, что мощность на гармониках, излучаемая объектом (а значит и эффективность обнаружения при прочих равных условиях), растет при увеличении мощности излучения локатора Ризл.., снижении частоты его излучения f и номера принимаемой гармоники N. Кроме того, чем ниже частота излучения локатора, тем меньшие значения имеют коэффициенты затухания K1, K2,

что также ведет к увеличению мощности сигнала от объекта.
Существенным отличием нелинейной локации от классического наблюдения (обнаружения) объектов с активным ответом является прямое преобразование падающей на объект энергии зондирующего сигнала в энергию высших гармоник.
В связи с этим модель радиолокационного наблюдения (обнаружения) в условиях нелинейной локации можно классифицировать как наблюдение с полуактивным ответом, что связано с отсутствием потребления энергии объектом от специального источника питания. Особенностями его являются очень малое значение коэффициента нелинейного преобразования ($\xi N << 1$) и зависимость его от частоты и мощности зондирующего сигнала локатора.
Определим понятие нелинейного объекта.
Нелинейным объектом называется объект, обладающий нелинейной вольт-амперной характеристикой (ВАХ) (рис.1). К ним относятся диоды, транзисторы, микросхемы, контакты металл-окисел-металл (МОМ-диод). К простейшему нестабильному МОМ-диоду относится и классическая двуокись железа - ржавчина. Специально созданные МОМ-диоды до середины 60-х годов использовались как детекторные диоды сантиметрового и миллиметрового диапазонов.
7
ВАХ любого нелинейного элемента разлагается в ряд Тейлора в виде апроксимирующего степенного полинома. Тогда выходной ток на воздействие гармонического входного сигнала будет иметь вид:

$$i_{вых.}(t) = i_0 + \alpha e_s(t) + \beta e^2_s(t) + \gamma e^3_s(t) + \dots . \qquad (2)$$

где $i_s(t)$ - входной сигнал на нелинейном элементе
Из (2) следует, что за счет нелинейности ВАХ в выходном сигнале за счет детектирования появляется постоянная составляющая e0, основная гармоника с амплитудой, умноженной на коэффициент a и высшие гармоники основной частоты, амплитуды которых пропорциональны соответствующим коэффициентам. Определим физическое понятие этих коэффициентов. Из [6] следует, что a есть крутизна ВАХ в рабочей точке.

$$\alpha = \left.\frac{di}{de}\right|_{e=E_0}$$

$$\beta = \left.\frac{1}{2!}\cdot\frac{d^2i}{d^2e}\right|_{e=E_0} = \left.\frac{1}{2!}\cdot\frac{d\alpha}{de}\right|_{e=E_0}$$

$$\gamma = \left.\frac{1}{3!}\cdot\frac{d^3i}{d^3e}\right|_{e=E_0} = \left.\frac{1}{3!}\cdot\frac{d^2\alpha}{d^2e}\right|_{e=E_0}$$

Коэффициенты β, γ являются соответственно первой и второй производными
от крутизны ВАХ в рабочей точке E0.
Большинство полупроводниковых приборов, используемых в радиоэлектронных устройствах съема информации - транзисторы, диоды, микросхемы, обладают характеристиками, близкими к квадратичной. Что касается естественных МОМ-диодов - ржавых частей металла или их контактов, идентификация строится на предположении кубической зависимости их ВАХ, когда в (2) отсутствуют производные четного порядка. Данное предположение не имеет под собой физических оснований, поскольку даже искусственными технологическими приемами невозможно создать идеальные квадратичную или кубическую зависимости ВАХ.
Естественный контакт двух металлов или ржавчина представляют собой элемент с механически нестабильным “p-n переходом”, а следовательно и с нестабильной ВАХ, которая в данном случае сильно зависит от всех параметров окружающей среды, что автоматически ведет к такой же чувствительности к внешним параметрам и крутизны и остальных ее производных.
Эффект затухания

Большинство специалистов основываются на "эффекте затухания" при распознавании полупроводникового и ложного соединения. Этот эффект проиллюстрирован на рис.3. Если вы слушаете демодулированный аудиоотклик от настоящего полупроводника, то по мере приближения к нему антенны уровень шумов будет значительно понижаться. И напротив, по мере удаления от него уровень шума начнет возрастать и постепенно вернется к нормальному. Демодулированный аудиосигнал достигает наименьшего значения непосредственно над полупроводниковым соединением и увеличивается до нормы в стороне от него.

При приближении антенны НЛ к ложному соединению, аудиошум может усилиться и достигнуть своего максимального значения непосредственно над ним или в некоторых случаях слегка уменьшиться. По мере удаления антенны НЛ аудиошум вернется к обычной норме.

Уровень аудиошума

Фундаментальная теория "эффекта затухания" достаточна проста.

Если НЛ излучает немодулированный сигнал, то сигнал отклика на частотах гармоники также будет немодулированным и будет наблюдаться эффект затухания.

Аудио демодуляция, необходимая для "эффекта затухания" может быть реализована как в НЛ с непрерывным так и с импульсным излучением (об этом будет сказано далее).

Существует несколько моделей НЛ российского производства, в которых реализован режим "20К", который основан на "эффекте затухания" и используется как способ распознавания типов соединений. Большинство ложных соединений легко распознаются проявляя "эффект затухания".

В НЛ «Катран» используется обычная частотная модуляция непрерывного излучения, что является более эффективным способом, использующим "эффект затухания".

Возможности применения аудиодемодуляции в НЛ

При применении НЛ в поисковых мероприятиях возможно не только обнаружение электронных устройств, но и их классификация при помощи аудио демодуляции. Так, например, при обнаружении некоторых записывающих устройств, можно услышать аудио сигнал записывающей головки. Более того, если НЛ дает хорошую аудиодемодуляцию, то зачастую возможно прослушивание синхронизирующих импульсов при обнаружении видеокамер. Используя частотную демодуляцию, иногда возможно прослушать характерные аудио сигналы в электронных устройствах, возникающих из-за фазовых сдвигов. Поэтому, очень важно иметь достаточный опыт работы с ЛН для распознавания электронных устройств по характерным аудио сигналам.

Кроме того, при обнаружении ложного соединения, можно без особого труда отличить его от полупроводника, прослушивая демодулированный аудио сигнал и одновременно производя на него физическое вибрационное воздействие, постукивая по стене кулаком или резиновым молотком. Ложное соединение отреагирует на подобное воздействие треском в наушниках. Чистый полупроводник при этом будет "молчать".

Использование FM-модулированного тона значительно расширяет пространственный диапазон обнаружения НЛ, в том случае, если его приемный тракт обладает качественным аудиодемодулятором и хорошей изоляцией от передающего канала. Однако, этот режим тональной модуляции не позволяет различать полупроводники от ложных соединений.

Импульсное или непрерывное излучение.

В зависимости от режима излучения нелинейные локаторы делят на локаторы с непрерывным и импульсным излучением.

Очевидно, что чем выше мощность излучения локатора, тем глубже проникает электромагнитная волна в облучаемую поверхность, и тем больше вероятность обнаружения помещенной в стену закладки. Но большая мощность излучения на высоких частотах оказывает вредное воздействие на оператора [53].

Для обеспечения его безопасности максимальная мощность излучения локатора в непрерывном режиме не должна превышать 3... 5 Вт [53]. При импульсном режиме мощность в импульсе достигает 300 Вт, однако, средняя мощность очень мала. Например, в локаторах серии "Циклон" максимальная средняя

мощность составляет 0,12 Вт, а локаторе "Октава" - от 0,45 Вт до 1,5 Вт [53].

Современные нелинейные локаторы имеют возможность изменения мощности зондирующего сигнала. Например, в локаторе NJE - 400 (непрерывного излучения) мощность регулируется в пределах от 10 мВт до 1 Вт, в Super Broom Plus (непрерывного излучения) - от 1 мВт до 3 Вт, а в локаторе "Циклон-М" (импульсный) - от 80 до 250 Вт. Причем в некоторых локаторах (например, в Super Broom Plus) мощность излечения устанавливается (снижается) автоматически в зависимости от мощности сигнала, принимаемого на второй гармонике, и тем самым предотвращается перегрузка приемника.

Приемники нелинейных локаторов с непрерывным излучением имеют чувствительность -120 ... 145 дБ, с импульсным - 110 ... 120 дБ и обеспечивают дальность обнаружения полупроводниковых элементов 0,5 ... 1 м и более. Максимальная глубина обнаружения объектов в маскирующей среде (строительных конструкциях) составляет десятки сантиметров. Например, локаторы серии "Циклон" обнаруживают радиоэлектронные изделия в железобетонных стенах толщиной до 50 см, в кирпичных и деревянных стенах - до 70 см [53].

В большинстве современных локаторов используются приемники с регулируемой чувствительностью. Например, в нелинейном локаторе "Энвис" диапазон регулировки чувствительности приемника составляет 45 дБ, а в NR-900E - 50дБ.

Точность определения местонахождения РЭУ составляет несколько сантиметров (например, в локаторах "Родник" и "Циклон" - 2 см).

Радиолокаторы «Родник-ПМ», «Переход», «Энвис», Super Broom и др. обеспечивают дополнительный режим прослушивания модулированных сигналов локатора, отраженных от полупроводниковых элементов закладок. Принцип модуляции аналогичен модуляции при высокочастотном навязывании [57, 62].

Современные нелинейные локаторы имеют небольшие размеры, вес и позволяют работать как от электросети, так и от автономных источников питания (аккумуляторов).

Например, у нелинейного локатора "Омега" вес приемо-передающего блока составляет 2 кг, а антенны со штангой - 0,8 кг. Вес нелинейного локатора "Циклон-М" в упаковке (кейсе) - 5,5 кг (при этом вес приемо-передающего блока составляет 1,2 кг). У нелинейного локатора Orion (NJE - 400) приемо-передающий блок и антенна закреплены на одной телескопической штанге, и общий вес конструкции не превышает 1,8 кг. Для удобства работы в этом локаторе используются беспроводные инфракрасные наушники.

Ряд закладных устройств выполняются по МОП- технологии, в экранированных корпусах. Поэтому их обнаружение даже с использованием нелинейных локаторов затруднено, так как уровень переизлученных сигналов на второй и третьей гармониках незначителен.

Большинство моделей НЛ, производимых в мире, используют непрерывное излучение (CW), т.е. излучают непрерывный узкополосный сигнал. Однако существуютНЛ, которые работают в импульсном режиме, что дает ряд преимуществ. Одно из них - меньшее потребление тока аккумуляторных батарей при хорошей конструкции передатчика. Таким образом, приемник принимает сигналы с частотой, приемлемой для восприятия человеческого слуха и зрения, в то время как передатчик выключается на значительные интервалы времени. Это позволяет уменьшить габариты и энергоемкость аккумуляторных батарей и источников питания. Кроме того, для использования эффекта затухания, описанного выше, НЛ непрерывного излучения обязательно должен иметь высококачественные малошумящие усилители в приемном тракте и хороший демодулятор для обеспечения качественного аудио. Еще одним методом аудиодемодуляции сигналов является импульсное излучение. Если частота следования импульсов выше порога частотного диапазона слышимости, то в этом случае для качественной демодуляции аудио сигнала достаточно простейшего АМ демодулятора.Не имеет значения, какой тип излучения использует НЛ импульсный или непрерывный, если он прост в обращении и обеспечивает хорошую аудио демодуляцию. НЛ «Катран» позволяет прослушать АМ и ЧМ аудио, используя импульсное излучение для амплитудной демодуляции и непрерывное для частотной, что максимально использует "эффект затухания".

Важно понимать, что при работе с НЛ имеют место 2 процесса:

1. Обнаружение нелинейного соединения.
2. Распознавание типа соединения (полупроводник или ложное).

При работе локатор должен иметь не только значительную дальность обнаружения, но и возможность регулировки его основных параметров (как правило мощность излучения или, как в случае с «Катраном» уровень интеграции цифровой обработки сигнала) для достижения необходимой глубины обнаружения в исследуемом материале.

Однако, не менее важно использовать методы анализа демодулированного аудио, основанные на эффекте затухания и вибрационном физическом воздействии.

Для максимальной надежности хороший НЛ должен иметь несколько способов определения различия между настоящим полупроводником и ложным соединением.

В «Катране» реализованы: режимы импульсного и непрерывного излучения, позволяющие достичь максимальной дальности обнаружения; сравнение уровней сигналов 2-й и 3-й гармоник; а также различные способы, позволяющие отличить полупроводник от ложного соединения.

В «Циклоне» реализован импульсный многочастотный режим

История создания нелинейных локаторов

Разработки нелинейных локаторов, получивших такое название из-за использования в своей работе нелинейных свойств полупроводниковых элементов, начались в США, Великобритании и СССР в середине 70-х годов. Первым устройством, поступившим на вооружение ЦРУ, был локатор "Super Scout", серийный выпуск которого начался с 1980 г. В 1981 г. появился британский "Broom", который несколько уступал американскому аналогу. Отечественный серийный локатор появился в 1982 г. и назывался "Орхидея". Еще раньше ему предшествовали несколько образцов, которые были сняты с появлением "Орхидеи" [53].

В настоящее время для поиска закладных устройств широко применяются нелинейные локаторы отечественного производства: "Обь", NR - 900E, "Родник - 23", "Энвис", "Циклон", "Переход", "Омега-3" и др., а также импортные локаторы: Super Broom, Orion (NJE - 4000), Super Scout и т.д. (рис. 2.29 ... 2.31).

Характеристики некоторых нелинейных локаторов приведены в таблице.

Название	Режим излучения	Мощность излучения, Вт		Средняя мощность, макс. Вт	Частота излучения, Мгц	Частота приема, Мгц	Напряжение питания, В	Габариты, см	Стоим. USD	M a,
		мин	макс							
Super Scout (США)	непр.	0,5	2	2	915	1830 2745	220,12	53x5x20	55000	18
Broom (Велико британия)	непр.	0,06	0,9	0,9	915	1830	220	51x24x8	45000	12
Diviner (Велико британия)	непр,		2,5	2,5	890	1780	12	35x17x7	25000	4,
Armashield (Велико британия)	непр.	0,3	3	3	888	1776 2664	12	28x25x5	18000	3,
PC-Elec t.ronik (Германия)	непр.	0,3	3	3	890	1780	220	55x45x18	45000	1
Обь (Россия)	непр.	0,5	3	3	1000	2000 3000	220	47x40x10	4500	1
HP - 900 (Россия)	имп.		100	0,25	900	1800	220,12	18x25x13	5900	8
Октава (Россия)	имп.	50	300	1,5	885	1770	220	16x15x5	5900	7
Циклон (Россия)	имп.	80	300	0,12	680	1360	220	45x36x9	7915	7,
Циклон-М (Россия)	имп.	80	300	0,12	680	1360	220/12	17x12x4	7325	2,
Циклон М1А (Россия)	имп.		250	0,09	680	1360	220/12	15x12x4	7325	1,

Что касается важности применения нелинейного локатора, то в настоящее время это единственное техническое средство, которое гарантирует почти 100 процентное качество обследования помещений по выявлению скрытых радиоэлектронных устройств.

Для поиска таких закладных устройств могут использоваться металлоискатели (металлодетекторы).

В металлоискателях используются магнитные и электрические свойства электропроводящих материалов, которые в той или иной степени присутствуют в закладных устройствах. Любая закладка содержит токопроводящие элементы: резисторы, индуктивности, соединительные проводники, антенну, корпус

элементов питания или металлический корпус закладки и т.п.

Принципы работы металлоискателей основаны на измерении и селекции изменений активной и реактивной составляющей напряжения, наводимого на измерительной катушке металлоискателя вихревыми токами в исследуемом объекте, или изменении активного и реактивного сопротивления катушки [63, 87, 98, 102]. Вихревые токи возникают при облучении объекта магнитным полем, создаваемым другой, так называемой поисковой катушкой металлоискателя. На эту катушку поступает аналоговый или импульсный сигнал от соответствующего генератора металлоискателя. Наводимые в приемной катушке сигналы усиливаются и анализируются встроенным в металлоискатель микропроцессором, обеспечивающим преобразование сигнала в ряд Фурье. Характеристики сигнала зависят от размеров токопроводящей поверхности объекта, коэффициента ее электропроводности, магнитной проницательности материала и частоты поля, которую подбирают в зависимости от решаемых задач.

В металлоискателях, применяемых для поиска закладок, частота составляет несколько кГц. Компенсация сигналов в измерительной катушке, возникающих в результате непосредственного действия мощного поля поисковой катушки, достигается за счет соответствующего пространственного расположения поисковой и измерительной катушек, использования компенсационной катушки с параметрами, идентичными параметрам измерительной, но с противоположным направлением намотки провода, или обеспечивается электронным путем [63].

Для обнаружения закладок применяются в основном ручные металлоискатели. Измерительная и поисковая катушки в них могут выполняться в виде торроида диаметром порядка 140 ... 150 мм, конструктивно объединенного с кожухом в виде ручки, в котором размещаются остальные узлы металлоискателя, или устанавливаться в едином кожухе металлоискателя.

Металлоискатели имеют звуковые и световые индикаторы, регулятор настройки чувствительности. Питание ручных металлодетекторов осуществляется от встроенных аккумуляторов.

Основная проблема, возникающая в металлодетекторах - подстройка коэффициента усиления под параметры среды. В современных металлодетекторах эта проблема решается микропроцессором, который обеспечивает автоматическую настройку его чувствительности.

Типовым представителем металлоискателей является портативный селективный металлодетектор "Унискан" [63]. Он представляет собой вихретоковый селективный металлодетектор с компенсированным вихретоковым преобразователем. Прибор имеет встроенную систему дискриминации (игнорирования) мелких ферромагнитных предметов (булавок, скрепок, иголок и т.п.).

Сигнализация обнаружения металлических предметов осуществляется выдачей сигнала на встроенный пьезоэлектрический излучатель и светодиодный индикатор. В случае обнаружения ферромагнитного объекта, прибор выдает монотонный звуковой сигнал частотой 2 ... 3 кГц, а в случае обнаружения объекта из цветного металла - прерывистый [63].

В приборе реализован динамический режим работы, то есть, обнаружение предмета происходит при перемещении детектора над этим предметом (рекомендуемая скорость перемещения - 50 см/с). Он позволяет обнаружить винт М 3 7 на дальности 8 см, а латунный диск 25·1 мм - на дальности до 17 см [63].

Металлодетектор имеет небольшие размеры (400·145·35) и весит 260 г [63].

3. МЕТОДИКА РАБОТЫ С НЕЛИНЕЙНЫМИ ЛОКАТОРАМИ

При проведении поисковых мероприятий вероятность обнаружения (или не обнаружения) закладных устройств напрямую зависит от возможностей используемого оборудования и наличия у поисковой бригады практического опыта по работе с ним.
Первый и главный признак – наличие электронной составляющей, или в упрощении p-n перехода, который является обязательным составным элементом любой электронной схемы. Транзистор, диод, микросхема– везде есть p-n переход.
При выполнении определенных требований (особенностей установки и изготовления) возможен пропуск закладного устройства при поиске его с помощью НЛ.
Например:
1. Изделие выполнено в корпусе, надежно изолирующем электронику от воздействий зондирующего сигнала. Если сигнал не получен элементом схемы, то соответственно, и откликов от него нельзя получить.
На сегодняшний день такие изделия не так часто встречаются, но все же они присутствуют на рынке специальных технических средств (СТС) и нельзя исключать возможность их применения.

Как пример можно привести несколько разработанных в России цифровых диктофонов в экранированных корпусах и уже появившиеся радио-закладки с исполнением фильтрации по антенному входу с экранированием корпуса.

2. Изделие установлено в электронное средство, легально размещенное в проверяемом помещении (например, радиозакладка в элементе питания кварцевых часов).

Способов обнаружения этих средств несколько:

• визуальный осмотр,
• рентгенография,
• сравнение с проверенным аналогом,
• контроль изменения различных физических параметров.

3. Изделие установлено в сложной помеховой обстановке. Например, в железобетонной стене за сеткой-рабицей (возможна установка электронного стетоскопа) выявление таких средств весьма сложно, так как НЛ получает смесь сигналов закладки и коррозийности сетки-рабицы.

4. При определенной ширине металлических конструкций (например, балки) зондирующий сигнал может отразиться от нее и не дойти до закладки. Выявление металлодетектором покажет прямую из металла, проходящую вдоль стены. Объект идентифицируется как балка.

Способы выявления – контроль за строительством объекта, постоянный мониторинг возможных технических каналов утечки информации.

5. Отсутствие в закладном устройстве, расположенном в проверяемом помещении, электронной составляющей, расположенной в зоне действия НЛ (например, микрофон типа СОМ, звуковод на удаленном окончании которого расположен микрофон с высококачественным усилителем. Способы обнаружения– тщательный визуальный осмотр проверяемого помещения.

6. Использование естественных каналов перехвата информации (радиотелефоны, вентиляционные шахты, ПЭМИН электронных средств). Способ выявления– оценка эффективности защищенности контролируемого помещения.

Одной из наиболее важных характеристик НЛ является его мощность, а точнее возможности глубины регулировки мощности и чувствительности. Большой диапазон таких регулировок дает возможность эффективно проводить работы в различных условиях помеховой обстановки.

В большинстве случаев приходится уменьшать мощность, чтобы «не поймать», например, телевизор, расположенный за двумя стенами.

4. «КАТРАН» - ПОРТАТИВНЫЙ ОБНАРУЖИТЕЛЬ ПОЛУПРОВОДНИКОВЫХ ЭЛЕМЕНТОВ

4.1 Введение

Портативный обнаружитель полупроводниковых элементов «КАТРАН» (в дальнейшем обнаружитель) предназначен для поиска и обнаружения электронных устройств, находящихся как в активном, так и в выключенном состоянии.

Работа обнаружителя основана на свойстве полупроводниковых элементов излучать вторую и третью гармоники при облучении их зондирующим СВЧ сигналом. Максимальный отклик от полупроводниковых элементов наблюдается на второй гармонике зондирующего сигнала. При облучении окисных пленок, образованных естественным путем, максимальный отклик наблюдается на третьей гармонике зондирующего сигнала.

Обнаружитель «КАТРАН» проводит анализ откликов облучаемых объектов как по второй, так и по третьей гармоникам зондирующего сигнала. Это позволяет надежно идентифицировать электронные устройства и естественные окисные полупроводники.

«КАТРАН» проводит автоматическое нахождение наилучшего частотного канала приема, свободного от помех, что позволяет работать с данным прибором даже в сложной электромагнитной обстановке.

Примененная цифровая обработка сигнала, позволяет оптимизировать алгоритмы обработки сигналов и получить максимальную чувствительность.

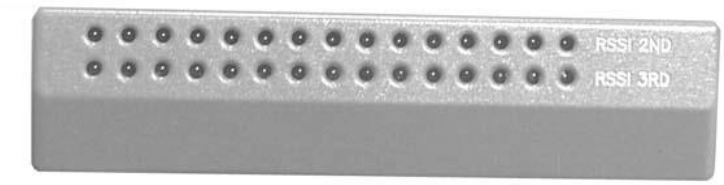
В обнаружителе предусмотрены различные виды модуляции излучаемых сигна-

лов:
• непрерывное излучение несущей частоты (рис.4.1а);
• частотная модуляция несущей частоты, FM = 1 кГц (рис.3.1б);
• импульсная модуляция несущей частоты со скважностью 3, fT = 1 кГц, τ = 0,3 мс (рис.3.1в).
Это даёт возможность не только обнаруживать электронные устройства, но и, при определенном навыке, определять их тип при прослушивании.
Рис. 4.1а Рис. 4.1б Рис. 4.1в
«КАТРАН» позволяет прослушивать работающие радиомикрофоны, в том числе и с прикрытием передаваемой информации, и использовать эффект акустозавязки для облегчения поиска.
4.2 Технические параметры
2.1. Виды излучаемого сигнала:
- непрерывное излучение несущей частоты фиксированная с шагом 0,5 МГц в диапазоне 890 895 МГц.
Выбор частоты осуществляется автоматически. Предусмотрена возможность излучения на несущей частоте, имеющей минимум помех в тракте приемника 2й гармоники
- импульсная модуляция несущей частоты со скважностью 3 (fT =1 кГц, τ=0,3 мс);
- частотная модуляция несущей частоты, FM = 1 кГц.
2.2. Максимальная мощность излучения в непрерывном режиме излучения не более 2 Вт.
2.3. Излучаемая мощность регулируется с помощью встроенного аттенюатора, имеющего четыре положения ……. 2 Вт; 0,6 Вт; 0,16 Вт; 0,08 Вт.
2.4. Реальная чувствительность радиоприемных устройств ……..не хуже минус 130 дБм.
2.5. Частоты настройки радиоприемных устройств равны удвоенной и утроенной частотам передатчика.
2.6. Динамический диапазон приемного тракта не менее……..…. 75 дБ.
4.3 Состав изделия и принадлежности.
Изделие состоит из блоков и устройств, перечисленных в таблице 1.
Наименование Кол-во
Приемо-передающий блок с пультом управления, зарядным устройством и ремнем для переноски.
Антенный блок.
Телескопическая штанга.
Сетевой блок питания.
Кабель питания от сетевого блока.
Аккумулятор (находится внутри приёмо-передающего блока)
4.4 Конструкция изделия
Пульт управления
Приемо-передающий блок
Блок антенн
Телескопическая штанга
Блок индикации

Внешний вид приёмо-передающего блока показан на рис. 4.4 и рис. 4.4а
Крышка аккумуляторной батареи
Разъём для

Подключения головных телефонов
Разъём для подключения шнура питания
Выключатель питания
Внешний вид сетевого блока питания показан на рис. 4.5 и рис. 4.6
Сетевой выключатель
Сетевой шнур
Разъем для подключения шнура питания
Предохранитель

4.5 Назначение основных узлов и блоков обнаружителя.
Приемо-передающий блок осуществляет:
1. Проверку работоспособности системы фазовой автоподстройки частоты (ФАПЧ) обнаружителя. При неисправности начинает мигать светодиод «TEST».
2. Анализ частотной загрузки радиоприемного устройства который проводится при каждом включении радиопередатчика обнаружителя. Поэтому во время работы при по- явлении мешающего сигнала (при работе в сложной электромагнитной обстановке) необходимо периодически выключать обнаружитель и включать его, тем самым осуществляя выбор оптимальной частоты излучения обеспечивающей наилучшую чувствительность и дальность обнаружения полупроводниковых элементов.
3. Формирование СВЧ-сигнала с выбранным видом модуляции.
4. Приём и цифровую обработку сигналов второй и третьей гармоники. Одновременная индикация уровней сигналов второй и третьей гармоник позволяет уверенно отличать сигналы искусственных полупроводников, входящих в состав электронных устройств, от естественных коррозийных, возникающих при окислении мест соединений различных металлов.
5. Демодуляцию откликов второй и третьей гармониках, усиление их до уровня, необходимого для прослушивания, как на наушники, так и на внутренний динамик. В обнаружителе предусмотрена возможность регулировки усиления на 20 дБ.
6. Прослушивание демодулированных сигналов осуществляется оператором поочередно.
7. Индикацию уровня сигналов второй и третьей гармоник.
8. Заряд и контроль функционирования внутренней аккумуляторной батареи.



Внешний вид блока индикации показан на рис. 4 7.
Красные светодиоды- 2-я гармоника
Зелёные светодиоды- 3-я гармоника

Пульт управления предназначен для выбора режимов работы обнаружителя.
Пульт управления состоит из корпуса, в котором расположена плата управления, кнопок управления режимами работы и светодиодов индикации режима работы.

Внешний вид пульта управления приведен на рис. 4.8.

Кнопки управления выполняют следующие функции:
VOL - регулировка уровня громкости демодулированного сигнала;
« + » - громче;
« - » - тише.
MODE - выбор режима работы передатчика и приемника:
AM – прослушивание демодулированного отклика второй
Рис. 4.8.
и третьей гармоники при зондировании объекта несущей с импульсной модуляцией;
FM –прослушивание демодулированного отклика второй и третьей гармоник при зондировании объекта несущей с частотной модуляцией;
CW –прослушивание демодулированного отклика второй и третьей гармоник при зондировании объекта немодулированной несущей;
RSSI – прослушивание в наушниках (динамике) щелчков, частота следования которых пропорциональна уровню сигнала от второй или третьей гармоники.
RX - выбор радиоприемного тракта.
2ND – радиоприемный тракт, анализирующий отклик 2 гармоники (включен если горит светодиод);
3RD - радиоприемный тракт, анализирующий отклик 3 гармоники (включен если горит светодиод);
- дискретная регулировка выходной мощности передатчика (0, 08 Вт; 0,16Вт; 0,6 Вт; 2 Вт)
Состояние работы аппарата отражают светодиоды:
TEST – сигнализация о неисправности работы изделия (если замкнуто кольцо ФАПЧ гетеродинов светодиод не горит);
BAT – сигнализация о состоянии аккумуляторных батарей.

4.6 Порядок работы

1. Для работы прибора от аккумуляторной батареи включить изделие «КАТРАН» выключателем питания на приемо-передающем блоке (см. рис. 4.4а).
2. Проконтролировать включение прибора по загоранию светодиодов, расположенных на пульте управления.
3. При необходимости прослушивания сигнала отклика на телефоны вставить в гнездо (см. рис. 4.4), расположенное на приемо-передающем блоке, штекер головных телефонов (телефоны в комплект поставки не входят).
4. Направить антенну в сторону от оператора.
5. Включить кнопкой TX минимальную мощность излучения. При этом автоматически выбирается канал приема с минимальным уровнем помех.
6. Установить на пульте управления необходимую мощность передатчика, режим излучения и режим работы радиоприемного устройства.
7. При наличии в контролируемом помещении электросети 220 вольт, рекомендуется подводить электропитание к изделию «КАТРАН» от сетевого блока, входящего в комплект поставки. Для этого одним концом (любым) присоединить кабель питания к разъёму питания сетевого блока (см. рис. 4.6), а другим концом присоединить кабель питания к разъёму питания приемо-передающего блока (см. рис.4.4).
8. Включить в электросеть 220 вольт сетевой блок питания.
9. Включить сетевой блок питания сетевым выключателем (см. рис. 4.5) и приемо-передающий блок выключателем питания (см. рис. 4.4а). При этом будет происходить автоматическая зарядка аккумуляторной батареи. Дальнейшую работу проводить согласно пунктам 2 … 6.

Нелинейный локатор “Циклон – М2Ч”

Малогабаритный двухчастотный нелинейный локатор для оперативно-поисковой работы.
Частоты излучения и приема находятся вне диапазонов работы сотовых телефонов стандартов GSM и NMT-450. На второй

гармонике реализован режим «3М» для селекции искусственных и естественных нелинейностей.
Предназначен для поиска скрытых в помещениях и автомобилях различных радиоэлектронных устройств съема информации. Обнаруживает любые магнитофоны, диктофоны, скрытые видеокамеры, любые модели сотовых телефонов и подслушивающие устройства, как в ручной клади, так и под одеждой. Обнаруживает радиоэлектронные устройства, находящиеся как во включенном, так и выключенном состоянии. В полевых условиях дальность обнаружения электронных устройств - до 10 м.
Позволяет обнаруживать взрывные устройства с электронным управлением подрывом, управляемые как по радиоканалу, так и с помощью внутреннего электронного таймера. При досмотре корреспонденции позволяет производить идентификацию по признаку - “электронное устройство”.
Не реагирует на металл!
Обнаруживает подслушивающие устройства:
– в железобетонных стенах толщиной 80 см;
– в кирпичных и деревянных стенах 150 см;
– в книжных шкафах без выемки книг;
– в столах и ящиках столов;
– под всеми видами полов.
Мировые аналоги отсутствуют. Разработан по А.С. SU №1832237

ОСНОВНЫЕ ПАРАМЕТРЫ	
Режим излучения	Двухчастотный, импульсный
Импульсная мощность излучения	120 - 150 Вт
Средняя мощность излучения	50 мВт
Мощность излучения, эквивалентная аналогу с одночастотным режимом	480 – 600 Вт
Чувствительность приемника	минус 115 дБВт
Глубина регулировки чувствительности	плавная, 60 дБ
Точность обнаружения объектов	± 1 см
Питание	»220В/=12В
Потребляемая мощность при $U_{пит.}$ = 12В	4 Вт
Масса в упаковке (в кейсе)	6 кг

Нелинейный локатор "Циклон - М1А"
Нелинейный локатор разработан и выпускается нашим предприятием ООО "ВИХРЬ". Конструкторская и технологическая документация на это изделие является собственностью ООО "ВИХРЬ" и не передавалась другим предприятиям.
Малогабаритный нелинейный локатор для оперативно-поисковой работы. Предназначен для поиска скрытых в помещениях и автомобилях различных радиоэлектронных устройств съема информации. Обнаруживает любые модели сотовых телефонов, магнитофоны, диктофоны, скрытые видеокамеры и подслушивающие устройства, как в ручной клади, так и под одеждой. Обнаруживает радиоэлектронные устройства, находящиеся как во включенном, так и выключенном состоянии. В полевых условиях дальность обнаружения электронных устройств - до 10 м. Позволяет обнаруживать взрывные устройства с электронным управлением подрывом, управляемые как по радиоканалу, так и с помощью внутреннего электронного таймера. При досмотре корреспонденции позволяет производить идентификацию по признаку - "электронное устройство".

Не реагирует на металл!
Обнаруживает подслушивающие устройства:
-в железобетонных стенах толщиной 50 см
-в кирпичных и деревянных стенах толщиной 70 см
-в книжных шкафах без выемки книг

-в столах и ящиках столов
-под всеми видами полов
Малый вес - 1,2 кг и наличие автономного питания - 12 В позволяет оператору работать длительное время в любых условиях.
По массогабаритным показателям и ТТХ не имеет аналогов.
ОСНОВНЫЕ ПАРАМЕТРЫ

Импульсная мощность излучения передатчика	250-300 Вт
Средняя мощность излучения передатчика	не более 100 мВт
Плотность потока мощности на расстоянии 20 см от антенны передатчика	Не более 2 мкВт/см2 (допустимая норма 10 мВт/см2)
Чувствительность приемника	минус 115 дБВт
Глубина регулировки чувствительности приемника	Плавная, 60 дБ
Точность обнаружения объектов	+1 см
Питание	220В/=12В
Потребляемая мощность при Uпит=12 В	1,5 Вт
Масса в упаковке (в кейсе)	4,5 кг

5. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

5.1 Содержание экспериментальной части работы

1. Убрать, по возможности, из контролируемого помещения, имеющиеся электронные устройства. Если этого сделать нельзя, то обследование необходимо вести при пониженной мощности излучения.
2. Установить максимальную выходную мощность и один из режимов работы приемника.
3. Расположить антенный блок параллельно обследуемой поверхности на расстоянии не более 10 см.
4. Медленно перемещая антенный блок, параллельно обследуемой поверхности и изменяя ориентацию антенн, проанализировать характер изменения принимаемого сигнала по второй и третьей гармоникам.
(В режимах ЧМ и АМ уровень громкости должен быть максимальным, в режиме «RSSI» частота повторения щелчков должна быть максимальной).
5. Анализ уровней принимаемого отраженного сигнала по второй и третьей гармоникам осуществляется по количеству зажженных светодиодов на соответствующей индикаторной шкале.
6. Удалите антенный блок от исследуемой поверхности или уменьшите выходную мощность и повторите измерения, изложенные в п.4. настоящей инструкции.
7. При обнаружении искусственного p-n перехода, как правило, наблюдается устойчивое свечение светодиодов индикатора по второй гармонике отраженного сигнала. При простукивании предполагаемого места нахождения p-n перехода, показания светодиодов не изменяются.
8. При обнаружении естественного p-n перехода, наблюдается устойчивое свечение светодиодов индикаторов по третьей гармонике отраженного сигнала.
При интенсивном постукивании по исследуемой поверхности показания индикаторов по третьей гармонике, как правило, изменяются.
Предложенная методика поиска не отражает всех нюансов, возникающих в конкретных случаях, и носит рекомендательный характер.
Основными задачами оператора при работе с НЛ являются, обнаружение, локализация и идентификация.
1. При поверке больших площадей рекомендуется предварительно начертить

на листах план-схему стен, потолка, пола, разбив его на квадраты (например, 50х50 см). Обнаружив отклик, отметьте на листе точку, где он наблюдался.
2. После обследования всего помещения займитесь идентификацией обнаруженных откликов. Рекомендация связана с тем, что необходимость постоянно прерывать локацию для визуального обследования объекта быстро утомляет оператора (если он работает один), утомляемость ведет к ухудшению внимания, а следовательно к возможному пропуску полученного отклика.

3. Для точного определения местоположения объекта используется метод постепенного уменьшения мощности и чувствительности НЛ.
4. Поймав отклик объекта, добейтесь получения максимального уровня принимаемого сигнала, плавно перемещая антенну.
После этого уменьшите мощность НЛ. При уменьшенной мощности повторите поиск точки с максимальным уровнем сигнала. В некоторых случаях возможно определение с точностью до 2–5 см, что вполне достаточно для последующего визуального обнаружения объекта.
4. После получения отклика от объекта необходимо принять решение, помеховый это сигнал или отклик p-n перехода.
Информация воспринимается из двух источников – на слух (из наушников) и визуально (две шкалы с уровнем сигналов на второй и третьих гармониках).
Если в наушниках прослушивается чистый тональный сигнал, и на шкале видно сильное превышение сигнала второй гармоники над третей, то объект идентифицируется как p-n переход.
5. После этого необходимо включить «выключенная модуляция» позволяет в случае работы закладного средства услышать характерные признаки (работу двигателей диктофонов, акустику проводного диктофона и т.д.).
Радиозакладка без закрытия канала передачи информации слышна не хуже, чем на обычном приемнике.
6. После обследования всего помещения необходимо идентифицировать обнаруженные отклики.
Следуя вышеописанной методике, произвести обследование макета на наличие нелинейных элементов и металлических изделий. Составить схему расположения обнаруженных элементов.
Наиболее сложным является поиск в неблагоприятной помеховой обстановке. Большое количество проводников, металлических изделий могут привести к обнаружению «коррозийного диода» или МОМ-диода (металл-окисел-металл).
Как отличить коррозийный диод или МОМ-диод от p-n перехода?
Если при простукивании объекта наблюдается треск, что нехарактерно при получении сигнала p-n перехода, то обнаружен МОМ-диод (например, ключи, скрепки, или монеты, положенные одни на другие). Для более качественно получения отклика рекомендуется использовать резиновый молоток.
Иногда после удара молотком МОМ-диод разрушается и сигнал пропадает. Например, часто в местах пересечения направляющих подвесных потолков происходит образование МОМ-диода. Достаточно легкого удара, чтобы его разрушить.
Еще одной сложностью при нелинейной локации, является наличие в помещении электронных средств. В некоторых случаях нет возможности вынести из помещения оборудование и его переносят из угла в угол. В таких условиях может появиться так называемый «призрак».
Вы наводите антенну на стену и получаете четкий отклик, который идентифицируется по всем признакам как p-n переход. Для убедительности обнаружения направьте антенну НЛ на обнаруженный объект под другим углом. Если сигнала нет, то возможной причиной его появления может стать компьютер, стоящий в трех метрах позади.
Внимание! Несмотря на направленную антенну, у всех НЛ существует задний лепесток диаграммы направленности. В некоторых случаях могут быть захвачены электронные средства, расположенные в четырех метрах позади. Передвиньте электронику в другое место, и, если сигнал пропал, то это «призрак», то есть прием сигнала полученного из-за наличия обратного лепестка диаграммы направленности.

Направив антенну на объект, с двух разных точек, можно определить, находится он непосредственно за стеной или на удалении.
Возможно, получение сигнала отклика при наводке зондирующего сигнала на проводные линии, в окончании которых находятся электронные средства.
Например, Вы можете поймать ретранслятор или телевизор, в который вставлена антенна, и сигнал наводится по коаксиальному кабелю. Достаточно выдернуть проводник из электронного устройства и сигнал пропадет.

6. МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С НЛ
1. Не направлять антенную систему в сторону глаз.
2. Избегать длительного пребывания людей в зоне главного лепестка диаграммы направленности антенной системы.
3. Не рекомендуется направлять НЛ на пожарные или охранные датчики, на работающие электронные средства, тем более возможные взрыватели, содержащие электронные схемы, так как возможно ложное срабатывание датчиков, выходу из строя электронных схем.

Лабораторная работа 5-7

Тема «Поиск каналов утечки информации с помощью индикатора поля. Поиск и обнаружение радиозакладок в помещении»

Место проведения : -класс 107
Цель работы: изучить методы противодействия несанкционированному съему информации с помощью радиозакладок, получить навыки практического использования данных методов.
Задача:
1. Изучить теоретический материал методики работы с индикаторами поля .
2. Получить задание на работу (см. Приложение).
3. Выполнить задание по поиску закладного устройства.
4. Составить отчет (см. Приложение)

Методы поиска радиозакладок с использованием индикаторов поля, интерсепторов и радиочастотомеров

Перед поиском **акустических радиозакладок** необходимо установить порог срабатывания (чувствительность) **индикатора поля**. С этой целью оператор, находясь в точке помещения на удалении нескольких метров от возможных мест размещения закладок (это, как правило, середина контролируемого помещения), должен установить регулятор чувствительности в такое положение, при котором световые или стрелочные индикаторы находятся на грани срабатывания или частота следования звуковых и световых импульсов была бы минимальной. Для этого он, сначала вращая регулятор добивается срабатывания индикаторов, а затем медленным вращением его в обратную сторону их выключает. Если регулятор уровня чувствительности отсутствует, то порог срабатывания устанавливают путем уменьшения длины телескопической антенны [58, 65, 66] .

При работе в сложной помеховой обстановке (например, в крупном городе) часто используются индикаторы поля, имеющие режекторные и полосовые фильтры [58]. Центральная частота режекторного фильтра, как правило, совпадает с частотой излучения одной из мощных станций, работающих в данном районе (телевизионной, радиовещательной, радиорелейной станции или центральной станции системы сотовой связи и т.д.). Выбором того или иного режекторного фильтра оператор добивается максимального ослабления помехового сигнала. Но при этом надо помнить, что частота радиозакладки может находиться в полосе режекции фильтра.

Полосовые фильтры осуществляют подавление принимаемых сигналов на частотах выше и ниже граничных частот фильтров и значительно повышают чувствительность индикатора поля. Но при этом время поиска значительно возрастает, так как обход помещения необходимо проводить столько раз, сколько используется полосовых фильтров.

Для активизации работы акустических радиозакладок, оборудованных системой VOX, в помещении необходимо создать тестовый акустический сигнал. В качестве источников тестового сигнала могут

использоваться любые источники звуковых сигналов (специальные акустические генераторы, магнитофоны, CD-проигрыватели и другие средства). Создать тестовый сигнал может и сам оператор, например, давая счет или постукивая пальцем по обследуемым предметам. Если требуется провести **поиск** закладных устройств **скрытно**, для создания тестового акустического сигнала целесообразно использовать средства, постоянно находящиеся в помещении. Наиболее часто в них используется радиоприемник, настроенный на частоту какой-либо радиовещательной станции.

В режиме скрытого поиска закладок рекомендуется отключить звуковую сигнализацию и устройство акустической "завязки" индикатора поля. Прослушивание детектированных сигналов необходимо осуществлять через головные телефоны [109].

Поиск акустических радиозакладок осуществляется путем последовательного обхода помещения, двигаясь вдоль стен и обходя мебель и предметы, находящиеся в помещении. При обходе помещения антенну необходимо ориентировать в разных плоскостях, совершая медленные повороты кисти руки и добиваясь максимального уровня сигнала. При этом расстояние от антенны до обследуемых объектов должно быть не более 5 ... 20 см. В процессе поиска динамик индикатора поля все время должен быть обращен в сторону обследуемых предметов или объектов. Обход помещения необходимо проводить два раза: первый с полностью выдвинутой телескопической антенной, второй - с антенной, выдвинутой на два колена [58].

При приближении индикатора к излучающей закладке напряженность электромагнитного поля возрастает, соответственно повышается и уровень сигнала на его входе. При превышении уровня сигнала порогового значения, устанавливаемого регулятором чувствительности, срабатывают световые или звуковой индикаторы, и при включении устройства акустической «завязки» появляется характерный сигнал самовозбуждения (свист). Уменьшая уровень громкости акустического сигнала в динамике, оператор может сузить зону, в которой возникает режим самовозбуждения (акустическая завязка), и тем самым локализовать место расположения закладки.

Необходимо помнить, что эффект акустической «завязки» наблюдается не у всех радиозакладок, поэтому основным демаскирующим признаком при их обнаружении является наличие излучения. В этом случае, локализация закладки с помощью индикатора поля осуществляется путем последовательного уменьшения чувствительности или длины антенны в зоне максимального уровня электромагнитного поля. Возможное местоположение радиозакладки определяется по максимальному уровню сигнала, при этом ошибка определения местоположения маломощных закладок (10 ... 20 мВт) составляет 5 ... 10 см.

Источником обнаруженного сигнала (электромагнитного поля) не обязательно является радиозакладка. В результате многочисленных переотражений электромагнитных волн внешних источников (мощных радиовещательных и телевизионных станций, ПЭВМ, оргтехники и т.п.) от стен помещения, различных металлических предметов и радиоаппаратуры распределение энергии в пространстве комнаты имеет сложный вид с минимумами и максимумами. Поэтому обнаружение закладки осуществляется **путем визуального осмотра** места (объекта), где уровень излучения максимален [3, 109].

Уменьшить количество подозрительных мест (объектов), подлежащих осмотру, позволяет использование индикаторов поля с селекцией сигналов, источники которых находятся в ближней зоне (то есть, когда R< 3·). К таким индикаторам поля относятся, например, детекторы HKG GD 4120 или Delta V/2 [126, 118].

Наиболее эффективны для выявления закладок индикаторы поля, имеющие амплитудные и частотные детекторы. Прослушивание через динамик или головные телефоны тестового акустического сигнала однозначно говорит о наличии радиозакладки.

Поиск радиозакладок с использованием индикаторов поля наиболее целесообразен и эффективен в местах с низким уровнем общего электромагнитного поля, то есть вдали от крупных городов, телевизионных, передающих центров, объектов с большой концентрацией мощных радиоэлектронных средств и т.п. (например, при удалении от города Москвы на расстояние свыше 20 ... 40 км). В этих условиях дальность обнаружения даже маломощной радиозакладки индикатором поля составляет несколько метров.

Процесс поиска радиозакладок с использованием индикаторов поля в крупных городах и местах с высоким общим уровнем электромагнитного поля очень трудоемкий и длительный по времени, так как в этих условиях дальность обнаружения маломощной радиозакладки не превышает 10 ... 50 см. Возникают неудобства с обследованием труднодоступных мест, например, потолка (особенно, если он высокий), люстр, воздуховодов и т.п.

Значительно облегчает поиск радиозакладок наличие **интерсепторов**, имеющих чувствительность значительно выше чувствительности детекторных индикаторов поля, память LOCKOUT и функцию блокировки частот (например "R 11") [127].

Методика поиска радиозакладок с использованием этих приборов заключается в следующем. Оператор, находясь в контролируемом помещении, включает тестовый акустический сигнал и включает интерсептор, который захватывает и детектирует наиболее мощный сигнал. Если детектированный и прослушиваемый с помощью динамика сигнал не соответствует тестовому, данная частота вводится оператором в память LOCKOUT и исключается из рабочего диапазона. Процесс продолжается до появления в динамике тестового сигнала (то есть до обнаружения излучения радиозакладки) или до пропадания всех сигналов (когда уровень оставшихся сигналов становится ниже чувствительности интерсептора).

При обнаружении излучения радиозакладки ее локализация осуществляется путем последовательного обхода помещения. В процессе поиска динамик интерсептора все время должен быть обращен в сторону обследуемых предметов или объектов. При приближении интерсептора к излучающей закладке на некоторое критическое расстояние появляется характерный сигнал самовозбуждения (акустической «завязки»). Уменьшая уровень громкости акустического сигнала в динамике, оператор может сузить зону, в которой возникает режим акустической "завязки", и тем самым локализовать закладку. Если интерсептор имеет индикатор уровня сигнала (например "Xplorer"), то возможное местоположение радиозакладки определяется по максимальному уровню сигнала.

Методика поиска радиозакладок с использованием **радиочастотомеров** аналогична методике поиска с использованием индикаторов поля. Поиск радиозакладок осуществляется путем последовательного обхода помещения. При обходе помещения антенну необходимо ориентировать в разных плоскостях, совершая медленные повороты кисти руки и добиваясь максимального уровня сигнала. Расстояние от антенны до обследуемых объектов должно быть не более 5 ... 20 см. При этом оператор фиксирует частоту принимаемого сигнала и его относительный уровень.

Радиочастотомер захватывает наиболее мощный в точке приема сигнал и измеряет его частоту. Знание частоты позволяет оператору грубо классифицировать принимаемый радиосигнал по возможным его источникам (радио- или телевизионное вещание, служебная связь, сотовая радиотелефонная связь и т. д). Как правило, радиочастотомер захватывает сигналы мощных радиовещательных станций (при этом при каждом измерении на жидкокристаллическом дисплее показания частоты меняются). При перемещении по комнате (в режиме автозахвата частоты) относительный уровень этих сигналов изменяется незначительно, и максимальный уровень наблюдается около оконных рам и труб парового отопления.

При приближении к радиозакладке на некоторое критическое расстояние сигнал от нее начинает превышать сигналы радиовещательных станций. Радиочастотомер захватывает этот сигнал и фиксирует его частоту. Наличие захвата сигнала радиозакладки подтверждается **стабильностью частоты сигнала** (при отключенной функции автозахвата частоты) и его высоким уровнем.

Возможное местоположение радиозакладки определяется по максимальному уровню сигнала. Обнаружение радиозакладки осуществляется путем визуального осмотра подозрительных мест и предметов.

Радиочастотомеры, имеющие высокоомные входы (например, ОЕ "М1" и ОЕ "3000А"), могут использоваться и для поиска закладок, передающих информацию по проводным линиям (линиям электропитания, телефонным линиям и т.д.) на высокой частоте. Для этого частотомер подключается к контролируемой линии с помощью щупа. При проверке линии электропитания частотомер подключается к нулевому проводу, который определяется обычным индикатором напряжения. Решение о наличии сетевой закладки в линии принимается при обнаружении в ней сигнала высокого уровня с высокой стабильностью частоты (при отключенной функции автозахвата частоты). Обычно частота передачи информации закладки лежит в пределах от 40 до 600 кГц, а в некоторых случаях - до 7 МГц. Поиск радиозакладки осуществляется путем визуального осмотра розеток, распределительных коробок и электрощитов, осветительных и электрических приборов (при осмотре они отключаются от сети и разбираются), а также непосредственно линий [3, 109, 110].

Аналогично поиску акустических радиозакладок осуществляется поиск телефонных радиозакладок.

При поиске **телефонных радиозакладок** необходимо снять телефонную трубку и поднести индикатор поля (интерсептор) к телефонному аппарату [109, 110]. При наличии в корпусе телефонного аппарата радиозакладки срабатывают световые или звуковой индикаторы поискового устройства, а в динамике или головных телефонах будет прослушиваться непрерывный тональный сигнал или короткие гудки телефонной станции. Радиочастотомером определяется частота закладки. Поиск телефонной закладки производится путем разборки и осмотра телефонного аппарата, телефонной трубки и телефонной розетки.

Далее поиск телефонных радиозакладок осуществляется путем последовательного обхода помещений вдоль телефонного кабеля [3, 109]. При обходе антенну необходимо ориентировать параллельно телефонной линии на минимально возможном расстоянии от нее. Особое внимание обращается на

распределительные коробки и места, где телефонная линия проложена скрытой проводкой. Осмотр проводиться вплоть до центрального распределительного щитка здания, который находится, как правило, на первом этаже или в подвале. При наличии на линии телефонной радиозакладки в месте ее расположения уровень сигнала поискового устройства будет максимален, а в динамике или головных телефонах индикатора поля или интерсептора будет прослушиваться непрерывный тональный сигнал или короткие гудки телефонной станции.

сновные характеристики индикаторов поля
Г 107 детектор поля

Назначение:

ST 107 детектор поля предназначен для обнаружения и локализации радиоизлучающих технических средств (РТС). К таким средствам, прежде всего, относят:
радиомикрофоны;
телефонные радиоретрансляторы;
радиостетоскопы;
скрытые видеокамеры с передачей информации по радиоканалу;
технические средства систем пространственного высокочастотного облучения;
радиомаяки систем слежения за перемещением объектов;
сотовые телефоны, радиостанции и радиотелефоны.

ST 107 Детектор поля отличается от **ST 007** дополнительными возможностями:

1. **Дополнительный частотный диапазон 2.5-7 ГГц за счет использования СВЧ антенны.**
2. **Повышенная пороговая чувствительность и точность измерения частотомера.**
3. **Улучшенная идентификация BLUETOOTH.**
4. **Идентификация сигнала 802.1g и базовый DECT.**
5. **USB порт.**
6. **Встроенный Li-Pol аккумулятор.**

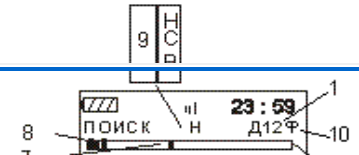
Принцип действия ST 107 основан на широкополосном детектировании электрического поля.

Индикатор поля ST107 имеет три основных режима работы:

Режим ПОИСК:

Данный режим предназначен для оперативного поиска и определения местоположения РТС. Использование данного режима основано на визуальной оценке уровня сигналов на 32 сегментной шкале, для каждого частотого диапазона. Дополнительно используется раздельная индикация непрерывного и имульсного видов сигналов,отображение идентифицированных сигналов - GSM, DECT, BLUETOOTH и 802.11g, а так же индикация частоты сигнала.

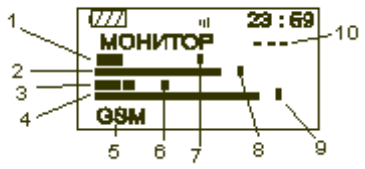
В индикаторе поля обеспечена возможность акустического контроля посредством головных телефонов или встроенного громкоговорителя.

	номера индицируемых диапазонов/кратковременная индикация установки нулевого уровня шкал.

		32-х сегментная шкала первого диапазона
		32-х сегментная шкала второго диапазона
		текущее абсолютное значение нулевого уровня шкалы первого диапазона в dB
		текущее абсолютное значение нулевого уровня шкалы второго диапазона в dB
	,5	индикация стабильной частоты радиосигнала
		индикация обнаружения радиочастотных сигналов **GSM, DECT, BLUETOOTH, 802.11G и** стабильной частоты радиосигнала
		индикатор уровня импульсной составляющей мощности источника радиоизлучения (ориентирована на импульсные радиопередатчики, такие как GSM, DECT и др.)
		Уровень интегральной мощности источника радиоизлучения (ориентирована на радиопередатчики с постоянно излучаемой мощностью)
		индикация выбранной чувствительности шкал индикации
	0	признак включения вильтра ВЧ

Режим МОНИТОРИНГ:

Предназначен для обнаружения РТС, по заданному порогу, частоте или виду сигнала. При автономной работе сохранение информации осуществляестя в энергонезависимой памяти изделия (9 банков по 999 событий).
Обеспечена работа по расписанию.

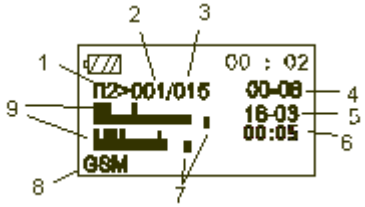


	,3	шкала индикации уровня непрывного сигнала РТС в первом и втором частотном диапазоне
	,4	индикация установленного уровня тревоги для непрывного сигнала в первом и втором частотном диапазоне.
	,7	шкала индикации уровня импульсного сигнала в первом и втором частотном диапазоне
	,9	индикация установленного уровня тревоги для импульсного сигнала в первом и втором частотном диапазоне
		индикация обнаружения радиочастотных сигналов **GSM, DECT, BLUETOOTH, WLAN** или стабильной частоты радиосигнала
	0	признак отсутствия/наличия разрешения записи в ПРОТОКОЛ СОБЫТИЙ.

Режим ПРОСМОТР ПРОТОКОЛА:

Предназначен для просмотра протокола событий произошедших в результате работы изделия в режиме МОНИТОРИНГ.
Обеспечена возможность сортировки событий по следующим признакам:
- времени наступления события;
- длительности события;
- уровню сигнала;
- диапазону.

Выбор данного режима осуществляется из МЕНЮ.
При отсутствии событий в протоколе индицируется надпись: "ПРОТОКОЛ ПУСТ"

	номер банка (1-9)
	номер просматриваемого события (001-999).
	общее число событий в банке (001-999).
	длительность события (часы/минуты, максимально 99ч 59мин)*
	часы и минуты начала события
	день и месяц события
	установленный порог тревоги
	индикация обнаружения радиочастотных сигналов **GSM, DECT, BLUETOOTH, WLAN или** стабильной частоты радиосигнала
	состояние уровней в момент события.

* В случае, если событие длилось менее одной минуты, то будет индицироваться знак «<1». При необходимости получения информации о длительность события с точностью до секунды воспользуйтесь программой «ST 107 DATA».

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Для работы с компьютером IBM PC используется специально разработанное программное обеспечение, предназначенное для :

- отображения в графическом виде результата работы индикатора поля ST 107 в режиме реального времени;

- загрузки и отображения, как в графическом, так и в текстовом формате результата работы ST 107 в режиме "Мониторинг" (протокол событий);

- полного управления ST 107 с ПК.

Для начала работы установите программное обеспечение с прилагаемого мини CD диска или с Интернет сайта производителя www.smersh.ru/manual/st107.shtml. Подключите основной блок к компьютеру с помощью прилагаемого USB кабеля. После запроса на установку драйвера укажите путь загрузки. При запросе на подтверждение установки ОБЯЗАТЕЛЬНО разрешите установку.

Технические характеристики индикатора поля ST-107	
Основной блок.	
Диапазон частот, МГц	50-7000
Диапазон 1, МГц	50-2500

Диапазон 2, МГц	2500-7000
Диапазон1	
Пороговая чувствительность по входу, не более, дБм	минус 75 (50 МГц) минус 73 (500 МГц) минус 70 (1500МГц) минус 65 (2000МГц) минус 50 (2500МГц)
Динамический диапазон индикации, дБ	55 (50-2000МГц) 40 (2000-2500МГц)
Чувствительность частотомера, дБм	минус 35 (50МГц) минус 50 (500МГц) минус 40 (1500МГц) минус 35 (2000МГц) минус 20 (2500МГц)
Погрешность измерения частоты, %	0.005
Частота среза ФНЧ, МГц	750
Затухание в полосе заграждения (больше 900МГц), дБ, не менее	30
Диапазон 2	
Пороговая чувствительность, Вт/см2	(2-9)*10-10
Динамический диапазон, дБ	45
Тип детектора	амплитудный, логарифмический
Полоса частот детектора	500кГц
Внутренний источник питания	Li-pol акк. батарея 3.6В
Потребляемый ток , мА, не более:	
Основной блок	80
СВЧ антенна	25
Габариты:	
Основной блок	90x54x21
СВЧ антенна	D=16, L=72
Вес основного блока, кг, не более	0.15

Комплектность поставки	
Наименование	Количество, шт
1. Основной блок	1
2. ВЧ антенна	1
3. СВЧ антенна (поставляется дополнительно)	1
4. Кабель USB	1
5. Зарядное устройство/блок питания	1
6. Мини CD	1
7. Техническое описание и инструкция по эксплуатации	1

* **Индикатор поля** (детектор поля) - это электронное устройство для индикации мощности электромагнитного излучения.

* **РТС** - Радиоизлучающие Технические Средства, такие как радиомикрофоны, радиоретрансляторы, радиостетоскопы, радиомаяки, радиостанции и радиотелефоны.

* **Поиск жучков** - процесс обнаружения и локализации РТС посредством измерения мощности электромагнитного поля индикатором поля.

ST 110 детектор поля

ST 110
Современный детектор поля, с возможностью подключения к ПК, идентификации каналов GSM, DECT, BLUETOOTH и 802.11g. С использованием СВЧ анетенны, диапазон частот до 7000МГц.

Назначение:

ST 110 детектор поля предназначен для обнаружения и локализации радиоизлучающих технических средств (РТС).
К таким средствам, прежде всего, относят:

- радиомикрофоны;
- телефонные радиоретрансляторы;
- радиостетоскопы;
- скрытые видеокамеры с передачей информации по радиоканалу;
- технические средства систем пространственного высокочастотного облучения;
- радиомаяки систем слежения за перемещением объектов;
- сотовые телефоны, радиостанции и радиотелефоны.

Основные улучшения ST 110 по сравнению с предыдущей моделью ST 107 состоят в следующем:

1. Цветной OLED дисплей
2. Режим САМОПИСЕЦ
3. Режим ОСЦИЛЛОГРАФ
4. Отключение встроенного Li-Pol аккумулятора при длительном хранении изделия.

Принцип действия ST 110 основан на широкополосном детектировании электрического поля.

Индикатор поля ST110 имеет два основных режима работы: ПОИСК и МОНИТОРИНГ. Дополнительными режимами являются Режимы ПРОСМОТР ПРОТОКОЛА и ОСЦИЛЛОГРАФ.

Режим ПОИСК:

Данный режим предназначен для оперативного поиска и определения местоположения РТС. Использование данного режима основано на визуальной оценке уровня сигналов на 32 сегментной шкале, для каждого частотого диапазона. Дополнительно используется раздельная индикация непрерывного и имульсного видов сигналов,отображение идентифицированных сигналов - GSM, DECT, BLUETOOTH и 802.11g, а так же индикация частоты стабильного сигнала. Обеспечена возможность акустического контроля

продетектированного сигнала посредством головных телефонов или встроенного излучателя.

1	32-х сегментный индикатор уровня импульсной составляющей мощности источника радиоизлучения (ориентирована на импульсные радиопередатчики, такие как GSM, DECT и др.
2	32-х сегментный индикатор интегральной мощности источника радиоизлучения (ориентирована на радиопередатчики с постоянно излучаемой мощностью)
3	выбранная чувствительность шкал индикации («Н»- низкая, «С»- средняя, «В»- высокая)
4	частотные диапазоны («Д1», «Д1Ф», «Д2» , «Д12» или «Д12Ф») /кратковременная индикация установки нулевого уровня шкал («НОЛЬ»)
5	текущее значение уровня для постоянной/импульсной составляющей сигнала относительно нулевого уровня, в dB
6	Значение частоты периодического сигнала, в МГц
7	Идентифицированные стандарты передачи данных (GSM, DECT, DECT BASE, BLUETOOTH или WLAN)
8	Изменение, во времени, уровня сигналов с преобладающей постоянной составляющей
9	Изменение, во времени, уровня сигналов с преобладающей импульсной составляющей
10	Текущее значение нулевого уровня для постоянной/импульсной составляющей сигнала

Режим МОНИТОРИНГ:

Предназначен для обнаружения РТС, по заданному порогу, частоте или виду сигнала. При автономной работе сохранение информации осуществляестя в энергонезависимой памяти изделия (9 банков по 999 событий). Обеспечена работа по расписанию.

1	Индикаторы уровня сигнала РТС
2	Графическое отображение уровней порогов тревоги
3	Признак отсутствия разрешения записи в ПРОТОКОЛ СОБЫТИЙ
4	обратный отсчет пятисекундного интервала при выборе данного режима
5	Текущее значение уровня для постоянной/импульсной составляющей сигнала относительно абсолютного уровня, в dB
6	Текущее значение уровня для постоянной/импульсной составляющей сигнала относительно абсолютного уровня, в dB

Режим ПРОСМОТР ПРОТОКОЛА:

Предназначен для просмотра протокола событий произошедших в результате работы изделия в режиме МОНИТОРИНГ. Обеспечена возможность сортировки событий по следующим признакам: времени наступления события, длительности события, уровню сигнала и частотному диапазону.

1	номер просматриваемого банка/Количество задействованных банков

2	номер просматриваемого события/количество событий в банке
3	Частотный диапазон в котором произошла тревога (Д1- 50-2500МГц, Д2 – 2500-7000МГц)
4	Параметры сигнала в момент превышения порога тревоги

Режим ОСЦИЛЛОГРАФ

1	Вариант установки (А - автоматическое Р - ручное) и относительное значение вертикальной развертки (от 1 до 7).
2	Осциллограмма
3	Значение горизонтальной развертки в пересчете на весь экран (от 1, 2,4,8, 16 и 32мс)

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Для работы с компьютером IBM PC используется специально разработанное программное обеспечение, предназначенное для :
- отображения в графическом виде результата работы ST 110 в режиме реального времени;
- загрузки и отображения, как в графическом, так и в текстовом формате результата работы ST 110 в режиме "Мониторинг" (протокол событий);
- полного управления ST 110 с ПК.

Технические характеристики индикатора поля ST-110	
Основной блок.	
Диапазон частот, МГц	50-2500
Пороговая чувствительность по входу, не более, дБм	минус 75 (50 МГц) минус 70 (1500 МГц) минус 50 (2500 МГц)
Динамический диапазон индикации, дБ	55 (50-2000 МГц) 40 (2000-2500 МГц)
Чувствительность частотомера, дБм	минус 35 (50 МГц) минус 50 (500 МГц) минус 20 (2500 МГц)
Погрешность измерения частоты, %	0.005
Частота среза ФНЧ, МГц	750
Внутренний источник питания	Li-pol акк. батарея
Потребляемый ток, мА, не более:	65
Габариты, мм	90x54x21
Вес, кг, не более	0.15
СВЧ анетенна – детектор ST110.SHF	
Диапазон частот, МГц	2000-7000
Пороговая чувствительность, Вт/см2	(2-9)*10-10
Динамический диапазон, дБ	45
Потребляемый ток, мА, не более	25
Габариты, мм	D=72, L=16

Комплектность поставки	
Наименование	Количество, шт
1. Основной блок	1
2. ВЧ антенна	1
3. ST110.SHF (поставляется дополнительно)	1
4. Кабель USB	1
5. Зарядное устройство/блок питания	1
6. Мини CD	1
7. Техническое описание и инструкция по эксплуатации	1

* Индикатор поля (детектор поля) - это электронное устройство для индикации мощности электромагнитного излучения.

* РТС - Радиоизлучающие Технические Средства, такие как радиомикрофоны, радиоретрансляторы, радиостетоскопы, радиомаяки, радиостанции и радиотелефоны.

* Поиск жучков - процесс обнаружения и локализации РТС посредством измерения мощности электромагнитного поля индикатором поля.

ДЕТЕКТОР ПОЛЯ ST 006 7

4 СОСТАВ ST 006
В комплект изделия входят следующие компоненты:
1. Основной блок.
2. Телескопическая антенна.
3. Зарядное устройство.
4. Техническое описание и руководство по эксплуатации.

4 ТЕХНИЧЕСКОЕ ОПИСАНИЕ И ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ

2 НАЗНАЧЕНИЕ
Детектор поля ST 006 предназначен для обнаружения и локализации в ближней зоне радиоизлучающих специальных технических средств (РСТС) негласного получения информации.
К таким средствам прежде всего относят:
· радиомикрофоны;
· телефонные радиоретрансляторы;
· радиостетоскопы;
· скрытые видеокамеры с радиоканалом передачи информации;
· технические средства систем пространственного высокочастотного облучения в радио*диапазоне;
· технические средства передачи изображения с монитора ПЭВМ по радиоканалу;
· радиомаяки систем слежения за перемещением объектов (людей, транспортных средств, гру*
зов и т. п.);
· несанкционированно включенные радиостанции, радиотелефоны и телефоны с радиоудлинителем;
ST 006 сохраняет работоспособность и соответствие параметров нормам технических условий при напряжении питания не ниже 3.2В, температуре окружающей среды от –20 до +35°С и влажности воздуха, не превышающей 95%.
Внимание! Входной усилитель ST 006 может быть выведен из строя высоким электростатическим напряжением, источником которого может являться накопленный электростатический заряд на синтетической одежде, коврах .

6 ТЕХНИЧЕСКОЕ ОПИСАНИЕ И ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ

3 ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ
Диапазон частот, МГц 30*2500
Чувствительность по входу, dBm, не хуже:
F = 30–800 МГц *56 (0.35мВ)
F = 800 –1700 МГц *50(0.71мВ)
F = 1700 –2500 МГц *42 (1.8мВ)
Динамический диапазон индикации, дБ 48
Диапазон звуковых частот, кГц 0.5 – 5.0
Источник питания аккумуляторная батарея 3.6В
Средний потребляемый ток, мА, не более 40
Габариты (без антенны), мм 85х53х19
Вес (без батареи), кг 0.15
ДЕТЕКТОР ПОЛЯ ST 006 7

4 СОСТАВ ST 006
В комплект изделия входят следующие компоненты:
1. Основной блок.
2. Телескопическая антенна.
3. Зарядное устройство.
4. Техническое описание и руководство по эксплуатации.

8 ТЕХНИЧЕСКОЕ ОПИСАНИЕ И ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ

5 УСТРОЙСТВО ST 006
Принцип действия ST 006 основан на широкополосном детектировании электрического поля.
Изделие обеспечивает прием радиосигналов в диапазоне от 30 до 2500 МГц, их детектирование и вывод для визуального и звукового контроля.
Уровень сигнала отображается на 16*сегментной светодиодной шкале. Предусмотрены отдельные индикаторы для сигналов стандартов GSM и DECT.
Для идентификации РСТС по характерному звуковому сигналу обеспечен режим акустической обратной связи.
Обеспечена индикация разряда аккумуляторной батареи и контроль состояния питания во время эксплуатации.

5.1 ОПИСАНИЕ КОМПОНЕНТОВ
5.1.1 Основной блок
Выполнен в виде малогабаритного моноблока (рис. 1).
ДЕТЕКТОР ПОЛЯ ST 006 9
На передней поверхности расположены:
– 17*сегментная светодиодная шкала (1);
– индикаторы обнаружения сигналов GSM и DECT (2).
На верхней поверхности установлено резьбовое отверстие для подсоединения телескопической антенны (3).
На правой поверхности расположены:
– кнопка управления (4);
– разъем для подключения зарядного устройства «CHARGE»(5).
На левой поверхности размещены:
– кнопка управления (6).
На задней поверхности размещены:
– декоративная решетка встроенного звукового излучателя (9);
– краткая инструкция по эксплуатации (8);
– шильд с информацией о производителе, модели и номере данного комплекта изделия (7).
10 ТЕХНИЧЕСКОЕ ОПИСАНИЕ И ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ

5.1.2 Зарядное устройство
Предназначено для заряда аккумуляторной батареи ST 006 от сети переменного тока 220В 50Гц.
5.2 УПАКОВКА

Для транспортировки и хранения компоненты изделия размещаются в прямоугольной коробке из гофрированного картона белого цвета размером 170x150x60 мм.
Для удобной и надежной укладки компонентов изделия предусмотрены пенополиуретановые прокладки.
Размещение компонентов изделия показано на рис. 2.
12 ТЕХНИЧЕСКОЕ ОПИСАНИЕ И ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ

6 РАБОТА С ST 006
Данный раздел описывает работу и не претендует на описание методики прове%
дения работ по обнаружению РСТС.
6.1 ОРГАНЫ УПРАВЛЕНИЯ И ИНДИКАЦИИ
6.1.1 ИНДИКАЦИЯ
Органы индикации расположены на передней панели изделия.
В верхней части расположена 17*сегментная светодиодная шкала
Первый сегмент синего цвета (PWR) индицирует включение питания (постоянное свечение) и разряд аккумуляторной батареи (мигание).
Основным назначением 16*сегментной светодиодной шкалы красного цвета является индикация уровня сигнала.
Последовательно загорающиеся сегменты индицируют усредненное значение мощности продетектированного сигнала, а одиночный сегмент его пиковые значения.

Лабораторная работа 8-10

Тема: Изучение средств выявления каналов утечки информации на примере программно-аппаратного комплекса измерения ПЭМИН «СИГУРД»»

Цель работы :

- **ознакомится с основными характеристиками и возможностями программно-аппаратного комплекса измерения ПЭМИН «СИГУРД»»**

Порядок выполнения работы

- ознакомится с представленным материалом;
- ответить на контрольные вопросы;
- оформить отчет.

Индикаторы электромагнитного поля и средства измерения побочных электромагнитных излучений и наводок (ПЭМИН)

1. Общие сведения

Принцип действия большинства *индикаторов электромагнитного поля* основан на широкополосном детектировании электрического поля. Индикаторы обеспечивают возможность *обнаружения* радиопередающих прослушивающих устройств с любыми видами модуляции.

Представленные на отечественном рынке комплексы для проведения специсследований позволяют в автоматическом режиме решать ряд задач *измерений побочных электромагнитных измерений и наводок* (ПЭМИН) и облегчают работу инженера-исследователя, повышают производительность его труда.

Некоторые комплексы на основе сканирующих приемников или анализаторов спектра *применяются для быстрого* анализа спектра ПЭМИН, излучаемых техническим средством, *но не обеспечивают высокой точности* измерений. При необходимости выдачи предписания на эксплуатацию технического средства, измерения, произведенные при помощи *таких* комплексов, подлежат обязательной ручной проверке с использованием метрологического измерительного оборудования (измерительных приемников или анализаторов спектра).

Комплексы типа «Навигатор» применимы для проведения *достаточно точных измерений* ПЭМИН в условиях экранированных помещений (безэховых экранированных камер), но результаты измерений могут быть достоверными только при их тщательной ручной проверке с использованием средств самого комплекса.

1. Автоматизация обнаружения гармонических составляющих тестового сигнала.

Обычно инженер-исследователь ищет гармонические составляющие на слух», распопознавая искомые компоненты по звуку и форме осциллограммы демодулированного сигнала. Инструментальная реализация такого режима приводит к тому, что автоматическая система, распознающая сигналы по их форме, работает лишь ненамного быстрее квалифицированного инженера-исследователя. Поэтому в первых комплексах данный режим не был реализован, а опознавание производилось *по критерию изменения уровней сигналов при включении тестового режима* на исследуемом техническом средстве (так называемый «энергетический критерий»). Такой способ дает неплохие результаты: вся работа по обнаружению сводится к двум проходам сканирования диапазона специсследования: при первом проходе запоминается картина шумов при выключенном тестовом режиме, при втором проходе исследуемое техническое средство переводится в тестовый режим, и измеряются уровни всех сигналов, превышающих запомненные шумы на заданное значение порога. Ускорение работы достигается очень существенное: вместо нескольких часов специсследование выполняется за считанные минуты. В результате инженер-исследователь получает таблицу частот и уровней сигналов (типичное количество обнаруженных составляющих – несколько сотен) и может рассчитать зоны разведдоступности. Однако результаты расчета могут оказаться неверными, так как электромагнитная обстановка изменяется со временем. В диапазоне от 9 кГц до 1000 МГц работают тысячи радиостанций и источников радиопомех. Некоторые из них время от времени включаются и выключаются, и если какой-то источник радиоизлучения не работал во время сканирования спектра шумов, а при втором проходе включился, его частота окажется в списке обнаруженных составляющих. Естественно, это может случайным образом изменить рассчитанные размеры зон разведдоступности.

Таким образом, оператору приходится вручную проверять все обнаруженные составляющие, на что будет уходить время. ***По-настоящему эффективно данный способ работает в безэховых экранированных камерах***, которые ввиду своей дороговизны доступны очень немногим предприятиям.

В более совершенных комплексах, одним из которых является «СИГУРД», применяется автоматическое опознавание информационных сигналов. Согласно методике инженеру исследователю

предлагается выполнить поиск какой-либо гармонической составляющей вручную или в специальном «полуавтоматическом» режиме, либо создать эталонный образ искомого сигнала при помощи редактора (генератора), либо выбрать ранее созданный образ из библиотеки, после чего комплекс автоматически обнаруживает в эфире сигналы, похожие на заданный сигнал. ***Для опознавания сигналов в таких комплексах применяется взаимно корреляционная функция***. Это более затратный по времени способ, но и существенно более точный.

2. Автоматизация измерения уровней сигналов

Этим свойством обладают практически все современные комплексы.

3. Измерение наводок в сети питания, линиях и коммуникациях Согласно действующим нормативным документам, измерение наводок в сети питания должно осуществляться при помощи эквивалента сети или пробников напряжения. Эквивалент сети достаточно сложное и относительно дорогостоящее устройство, однако измерения, проведенные с его помощью, обычно точнее измерений, выполненных с помощью пробника напряжения. «Чистая» сеть, имитируемая эквивалентом сети, позволяет измерять создаваемые исследуемым техническим средством наводки в сеть питания, уровень которых на 4–6 дБ выше собственных шумов эквивалента сети, в то время как точность измерений, выполняемых при помощи пробника напряжения, зависит от уровней шума сети питания. Для автоматизированных измерительных систем очень важна возможность использования в своем составе различных приемных устройств: антенн, пробников напряжения, эквивалентов сети. Соответственно, в программном обеспечении комплекса должен быть предусмотрен механизм поддержки дополнительных приемных устройств, а именно, возможность ввода таких параметров, как рабочий диапазон, антенные коэффициенты (коэффициенты затухания или усиления) и их автоматический учет в процессе измерений.

Таким механизмом обладают комплексы «Легенда» и «Сигурд».

2. Комплекс измерения ПЭМИН «СИГУРД»

Программно-аппаратный комплекс «СИГУРД» (рис. 5) представляет собой ***одну из самых совершенных систем*** оценки защищенности технических средств по каналу ПЭМИН и предназначен для проведения специальных исследований различных технических средств по выявлению, распознаванию и измерению сигналов их побочных электромагнитных излучений с максимальной степенью автоматизации процедур.

Система создана на базе анализатора спектра фирмы IFR (MARCONI) или других производителей, стандартного IBM-совместимого персонального компьютера (настольного или Notebook) и комплекта антенн. Могут быть применены любые антенны, предназначенные для работы в диапазоне от 9 кГц до 2 ГГц. Рекомендуется применение активных широкополосных антенн.

Антенный коэффициент вводится в управляющую программу и учитывается автоматически при выборе соответствующей антенны. Замена антенн в процессе измерений осуществляется оператором в соответствии с сообщениями управляющей программы.

Основным отличием данной системы от аналогичных разработок является четырёхэтапное обнаружение и измерение сигналов и полностью автоматическое, адаптивное распознавание частот (сигналов) ПЭМИН и автоматическое дистанционное управление параметрами тест-режимов на исследуемой ПЭВМ (на базе типового IrDA канала).

Рис. 5 Программно-аппаратный комплекс «СИГУРД»

1. На первом этапе выполнения задания в автоматическом режиме осуществляется фильтрация всех входных сигналов по энергетическому критерию (превышение на заданную величину над уровнем шумов).

2. Далее система выполняет коррекцию каждого выявленного сигнала, уточняя его частоту.

3. На третьем этапе осуществляется корреляционный двухступенчатый анализ сигналов в сравнении их с эталоном, хранящимися в файловой библиотеке. Эталон сигнала синтезируется оператором по спектрограмме реального сигнала в процессе формирования задания. Предусмотрено выделение сигналов, корреляционные характеристики которых не позволяют программе сделать однозначный вывод, и выдача их на экран оператору для принятия решения.

4. На последнем этапе выполняется измерение выявленных «опасных» сигналов.

Все спектры, зафиксированные в процессе специальных исследований, могут быть сохранены для последующего анализа. Данная функция позволяет дополнительно вести анализ спектров методом «наложения», при котором сравниваются два спектра, снятых в разных режимах работы исследуемого устройства. Изменения спектра по сравнению с сохранённым при наложении выделяются цветом.

Управляющая программа позволяет управлять всеми необходимыми режимами работы анализатора спектра. Все задаваемые оператором параметры запоминаются в виде «задания». Библиотека заданий сохраняется для последующего использования, в том числе любое задание может быть использовано в последующем без изменений или с любыми изменениями.

Выполнение любого задания может быть приостановлено оператором в любой момент и продолжено или запущено сначала или продолжено с изменёнными в случае необходимости параметрами.

Предусмотрен и ручной режим работы с анализатором спектра при управлении всеми его функциями от компьютера. Анализатором спектра можно управлять и автономно с помощью его органов управления. При этом при возврате под управление компьютера оператор может продолжить выполнение задания с параметрами, предусмотренными заданием или с введёнными с пульта управления анализатора спектра вручную.

Задача расчёта требуемых параметров исследуемых устройств решается отдельным программным модулем, использующим результаты измерений ПЭМИН исследуемого устройства в виде файла данных и дополнительные данные, вводимые оператором. ***Итогом расчёта является таблица данных измерений и расчётов, предназначенная для включения в отчёт***.

Анализатор спектра может работать непрерывно от автономного источника электропитания до полутора часов, что позволяет в ряде случаев минимизировать уровень помех при измерениях. Рекомендуемые измерительные антенны также предусматривают автономное электропитание. Таким образом, при использовании компьютера «Notebook», весь комплекс может быть мобильным и автономным.

Электромагнитные каналы утечки информации ТСПИ

К побочным электромагнитным излучениям технических средств передачи и обработки информации (ТСПИ) относятся:

• излучения элементов ТСПИ;

• излучения на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;

• излучения на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Электромагнитные излучения элементов ТСПИ. В ТСПИ, в частности и в линиях связи, входящих в их состав, носителем информации является электрический ток, характеристики которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по проводникам ТСПИ вокруг них в окружающем пространстве возникает электрическое и магнитное поле. По этой причине элементы ТСПИ можно рассматривать как излучатели электромагнитного поля, составляющие которого модулированы также по закону изменения информационного сигнала.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования.

Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электромагнитные излучения персональных компьютеров.

Согласно оценочным данным по каналу ПЭМИН (побочных электромагнитных излучений и наводок) может быть перехвачено не более 1–2 процентов данных, обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ) [33]. На первый взгляд может показаться, что этот канал менее опасен по сравнению, например, с акустическим, по которому из помещения может быть перехвачена речевая информации в полном объеме. Но необходимо помнить, что в настоящее время наиболее важная информация, содержащая коммерческие технологические секреты, обрабатывается на персональных компьютерах.

Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата – это данные, вводимые с клавиатуры компьютера или отображаемые на мониторе.

Компьютеры порождают электромагнитные излучения, которые не только создают помехи для радиоприема, но также создают технические каналы утечки информации. Соединительные кабели (линии связи), обладающие индуктивностью и емкостью, образуют резонансные контуры, излучающие высокочастотные электромагнитные волны, модулированными сигналами данных.

Аналогичная ситуация имеет место и при взаимном обмене сигналами между параллельно проложенными кабелями. ***Исследователями продемонстрировано восстановление сетевых данных через телефонную линию, причем телефонный кабель проходил рядом с кабелем компьютерной сети всего на протяжении двух метров.*** Еще одна опасность исходит от "активных" атак (высокочастотное навязывание): ***злоумышленник, знающий резонансную частоту, например, кабеля клавиатуры персонального компьютера, может облучать его на этой частоте,*** а затем регистрировать коды нажатия клавиш в ретранслируемом резонансном сигнале благодаря вызванным ими изменениям импеданса.

Для ПК высокочастотные излучения находятся в диапазоне до 1 ГГц с максимумом в полосе 50–300 МГц. Широкий спектр обусловлен наличием как основной, так и высших гармоник последовательностей коротких прямоугольных информационных импульсов. К появлению дополнительных составляющих в побочном электромагнитном излучении приводит также применение в вычислительных средствах высокочастотной коммутации.

Говорить о какой-либо диаграмме направленности электромагнитных излучений ПК не имеет смысла, так как расположение его составных частей имеет много комбинаций. **ПК имеет линейную поляризацию**. Она определяется расположением соединительных кабелей, являющихся основными источниками излучений в ПК с металлическим кожухом на системном блоке.

Уровни побочных электромагнитных излучений ВТ регламентированы по условиям электромагнитной совместимости целым рядом зарубежных и отечественных стандартов. Так, например, согласно публикации «№ 22 CISPR (специальный международный комитет по радиопомехам) **для диапазона 230–1000 МГц уровень напряженности электромагнитного поля, излучаемого оборудованием ВТ, на расстоянии 10 м не должен превышать 37 дБ.** Однако излучения такого уровня могут быть перехвачены на значительных расстояниях. *Следовательно, соответствие электромагнитных*

излучений средств ВТ нормам на электромагнитную совместимость не обеспечивает сохранение конфиденциальности обрабатываемой в них информации.

Электромагнитные излучения на частотах работы ВЧ генераторов ТСПИ и ВТСС. В состав ТСПИ и ВТСС могут входить различного рода высокочастотные генераторы как-то: **задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных устройств, генераторы измерительных приборов и т.д.**

При внешних воздействиях информационного сигнала (например, электромагнитных полей) на элементах ВЧ генераторов индуктируются электрические сигналы. Приемными антеннами для магнитного поля могут служить катушки индуктивности колебательных контуров, сглаживающие дроссели в цепях электропитания и т.д. Приемниками электрического поля являются провода высокочастотных цепей и другие элементы. Индуктированные электрические сигналы могут вызвать модуляцию собственных ВЧ колебаний генераторов и излучение их в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ ТСПИ. Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи т.п.) возможно за счет преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные в результате фазового сдвига сигнала обратной связи на определенных частотах, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения находится в пределах рабочих частот элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т.п.), переходящих в нелинейный режим работы при перегрузке за счет действия положительной обратной связи. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными за пределами контролируемой зоны.

Зона, в которой возможен перехват побочных электромагнитных излучений с помощью разведывательного приемника с последующей расшифровкой содержащейся в них информации (т.е. зона, в пределах которой отношение «информационный сигнал/помеха» превышает допустимое нормированное значение), называется опасной *зоной 2.*

Контрольные вопросы

1. Виды средств обнаружения радиозакладных устройств.
2. Перечислите основные устройства выявления побочных электромагнитных излучений.
3. Перечислите известные Вам программно-аппаратные комплексы для измерения ПЭМИН.
4. Типовой состав автоматизированных комплексов радиомониторинга.
5. Технические возможности комплексов радиомониторинга.
6. Какие характеристики электромагнитного поля определяются в выявленных побочных электромагнитных излучениях?
7. В каких расчетах используются характеристики электромагнитного поля побочных электромагнитных излучений?
8. В чем принципиальное отличие между программно-аппаратным комплексом радиомониторинга на основе сканирующего приемника и программно-аппаратным комплексом по оценке ПЭМИН?

Лабораторная работа № 11-12

Взлом моноалфавитного подстановочного шифра методом частотной атаки

Цель работы: ознакомиться на практике с использованием частотной криптоатаки при взломе подстановочных шифров.

Исходные данные:

Зашифрованный текст, перечень наиболее часто встречающихся букв в тексте, перечень наиболее часто используемых в русском языке букв.

Выходные данные:

Расшифрованный текст.

Теоретические основы:

Моноалфавитный подстановочный шифр - шифр, в котором каждой букве исходного алфавита поставлена в соответствие одна буква шифра.

Например, возьмем слово «КУКУРУЗА». Пусть букве «К» текста соответствует буква «А» шифра, букве «У» текста соответствует буква «Б» шифра, букве «Р» текста соответствует буква «В» шифра, букве «З» текста соответствует буква «Г» шифра, букве «А» текста соответствует буква «Д» шифра. После подстановки букв шифра вместо букв исходного теста слово «КУКУРУЗА» в зашифрованном виде будет выглядеть как «АБАБВБГД».

Недостатком подобного шифрования является то, что, если какая-то буква встречается в исходном тексте чаще всего (например, буква «О» в русском алфавите), то и соответствующая ей буква шифра в зашифрованном тексте также встречается чаще всего.

В нижеприведенной таблице приведены частоты встречаемости букв в английском тексте (в процентах):

Высокая		Средняя		Низкая	
E	12,31	L	4,03	B	1,62
T	9,59	D	3,65	G	1,61
A	8,05	C	3,20	V	0,93
O	7,94	U	3,10	K	0,52
N	7,19	P	2,29	Q	0,20
I	7,18	F	2,28	X	0,20
S	6,59	H	2,25	J	0,10
R	6,03	W	2,03	Z	0,09
H	5,14	Y	1,88		

Зная частоты наиболее встречающихся букв и подсчитав, какие буквы чаще всего встречаются в шифровке, криптоаналитик может подобрать расшифровку для некоторых букв текста. Затем, анализируя короткие слова, найти еще буквы, истинные значения которых можно с высокой степенью уверенности предугадать. Например, если уже расшифрована буква «О» и в тексте есть слово «ОЫО» (подчеркнуты уже расшифрованные буквы), то, скорее всего, шифру «Ы» соответствует буква «Н» в исходном тексте («ОНО»). Чем дальше расшифровывается текст, тем легче идет процесс расшифровки.

Методические указания

1. Запустить на выполнение файл labw01.exe
   На экране появится окно выполнения лабораторной работы (рис. 1):

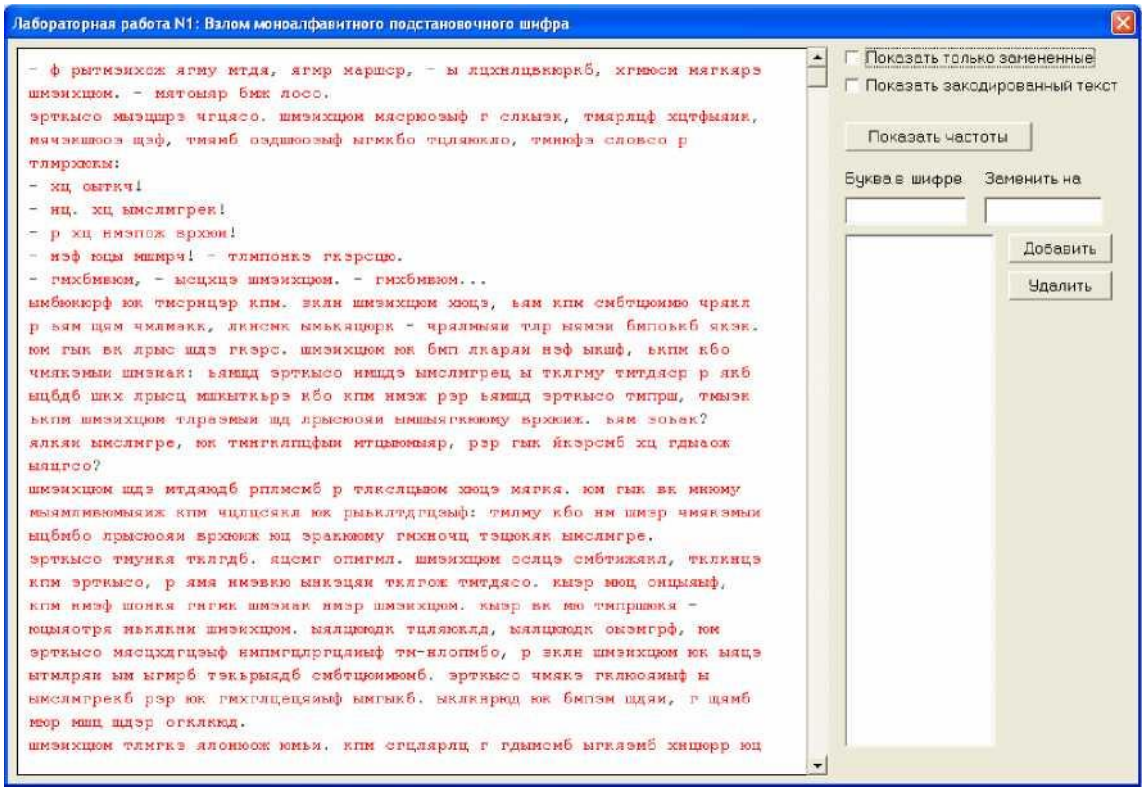


Рисунок 1. Окно выполнения лабораторной работы

В левой части окна находится зашифрованный текст (буквы, выделенные красным цветом). В процессе расшифровки расшифрованные (правильно или неправильно) буквы текста меняют цвет с красного на черный.

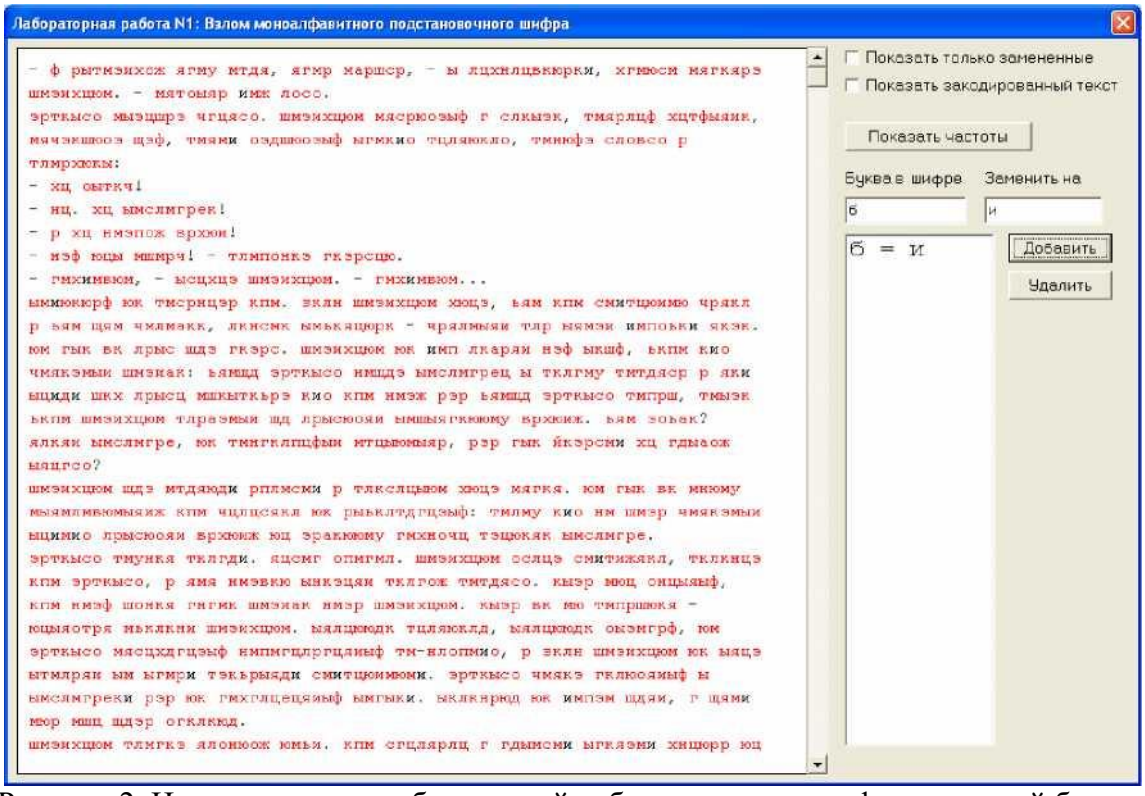


Рисунок 2. Изменения окна лабораторной работы после расшифровки одной буквы

Чтобы указать для какой-либо буквы шифра ее истинное (расшифрованное) значение, нужно в поле «Буква в шифре» указать значение буквы, например, “б”, а в поле «Заменить на» - ее истинное значение, например, “и”, а затем нажать кнопку “Добавить“. Результат такого действия приведен на рис. 2.

На рис. 3. Приведено окно выполнения лабораторной работы после добавления расшифровок нескольких букв.

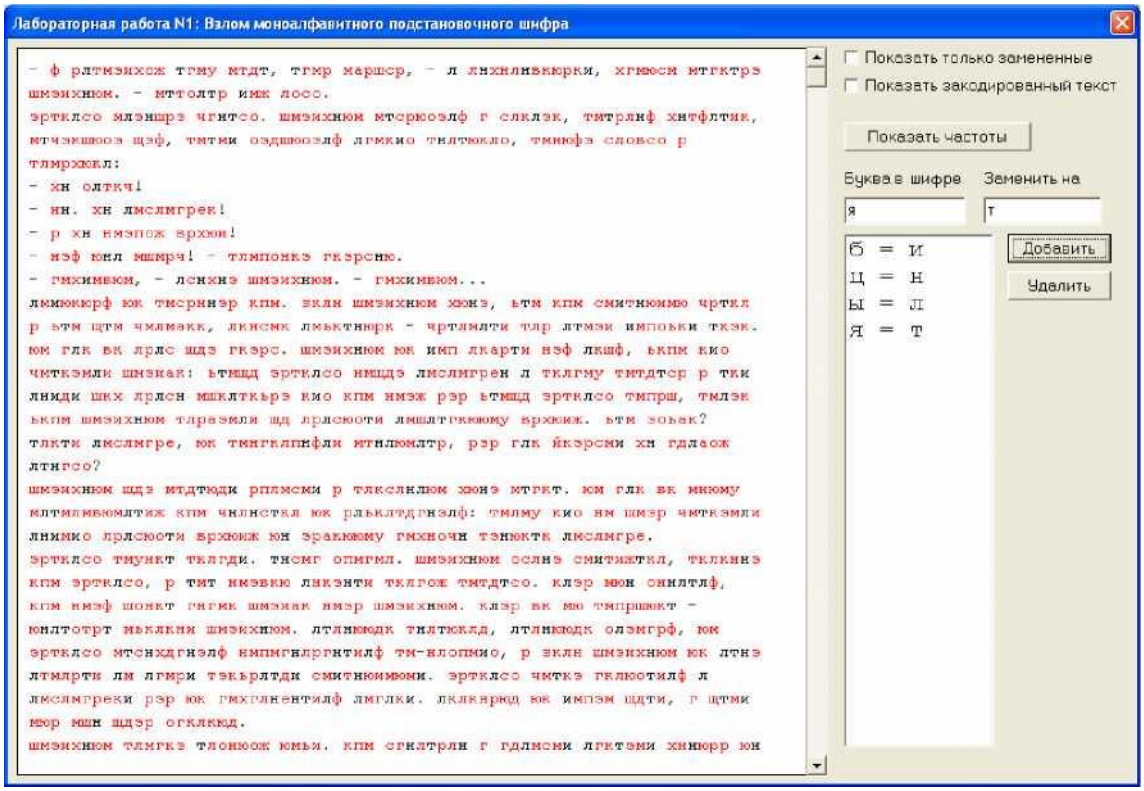


Рисунок 3. Окно лабораторной работы после расшифровки нескольких букв

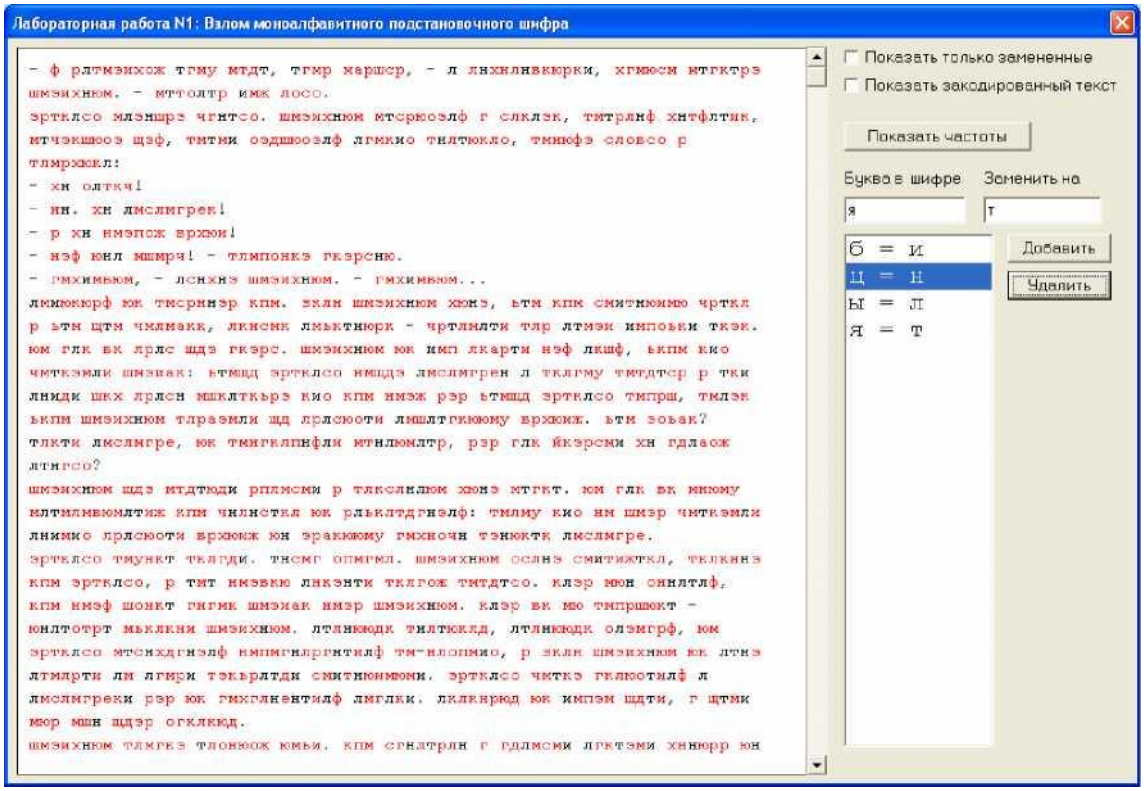


Рисунок 4. Процедура удаления ошибочно указанных расшифровок

Чтобы отменить указанную расшифровку буквы, нужно в списке расшифровок мышкой указать соответствующую пару букв и нажать кнопку «Удалить» (рис. 4).

Полоса вертикального скроллинга служит для навигации по расшифровываемому тексту.

2. Начинается частотная атака с анализа частот встречаемости букв в шифровке. Для этих целей в окне выполнения лабораторной работы предусмотрена кнопка «Показать частоты». При ее нажатии на экран выводится перечень десяти наиболее часто встречаемых букв в шифре, а также перечень букв, наиболее часто встречаемых в русском языке (рис. 5).

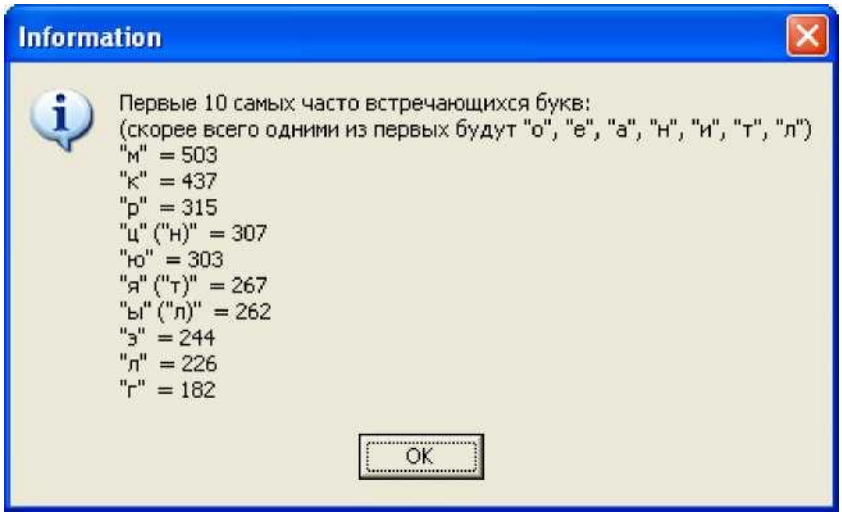


Рисунок 5. Информация о частотах встречаемости букв в шифре

Первым шагом в расшифровке текста может быть указание расшифровки для самой часто встречаемой буквы - буквы «о». Для случая, приведенного на рис. 5, указывается «о» как расшифровка буквы «м» шифра (см. рис. 6).

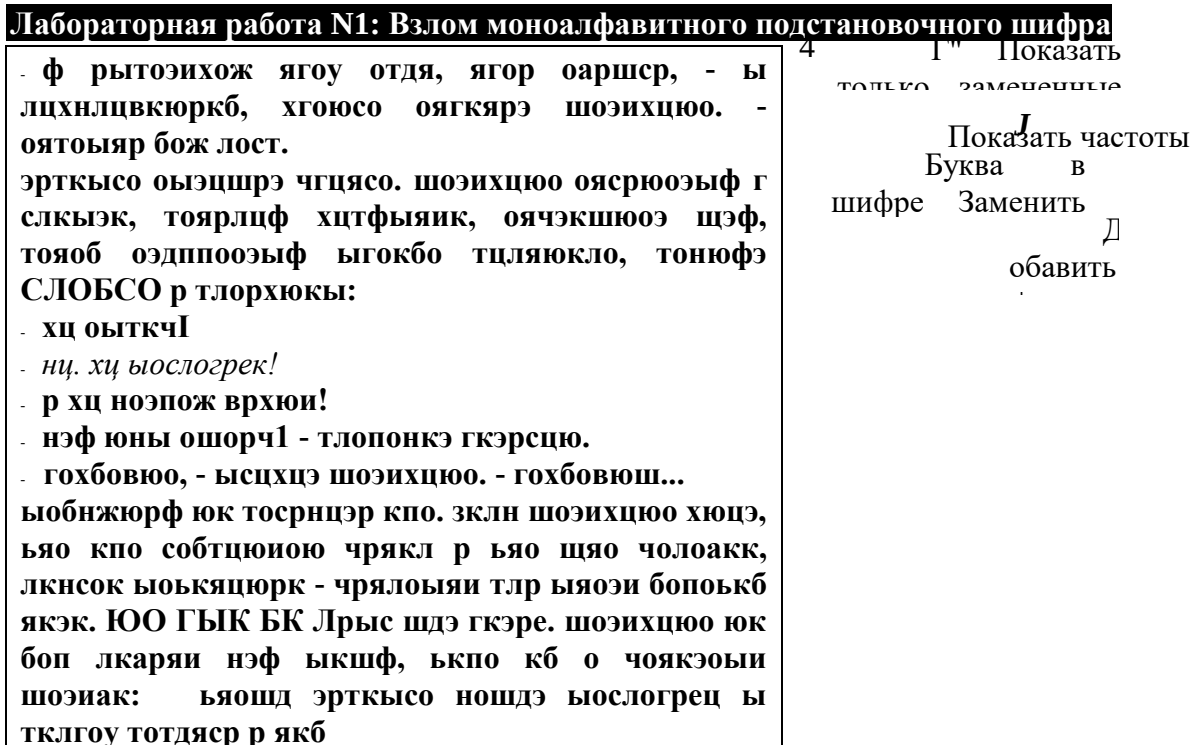


Рисунок 6. Первый шаг расшифровки - указание расшифровки буквы «о»

Следует помнить, что для конкретного текста частота встречаемости букв может быть несколько иной, чем в среднем для русского языка. Если в русском языке, например, буква

«т» встречается чаще, чем буква «л», то в каком-то конкретном тексте буква «л» вполне может встречаться чаще буквы «т». Поэтому слепо опираться на данные частотного анализа не следует.

3. В зашифрованном тексте осуществляется поиск коротких слов, зашифрованные буквы которых можно предсказать по уже расшифрованным буквам и частотной информации из рис. 5. На рис. 7. в верхней строчке есть фрагмент текста « ою », где «о» уже известно

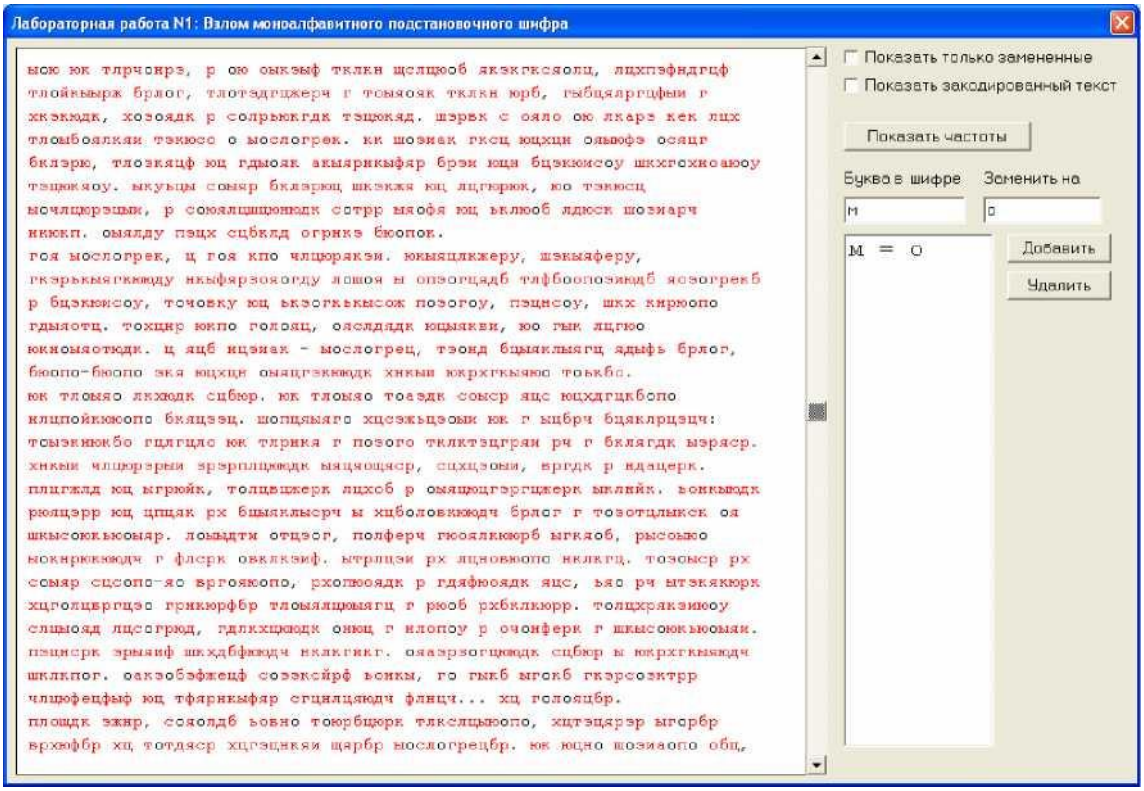


Рисунок 7. Поиск коротких слов

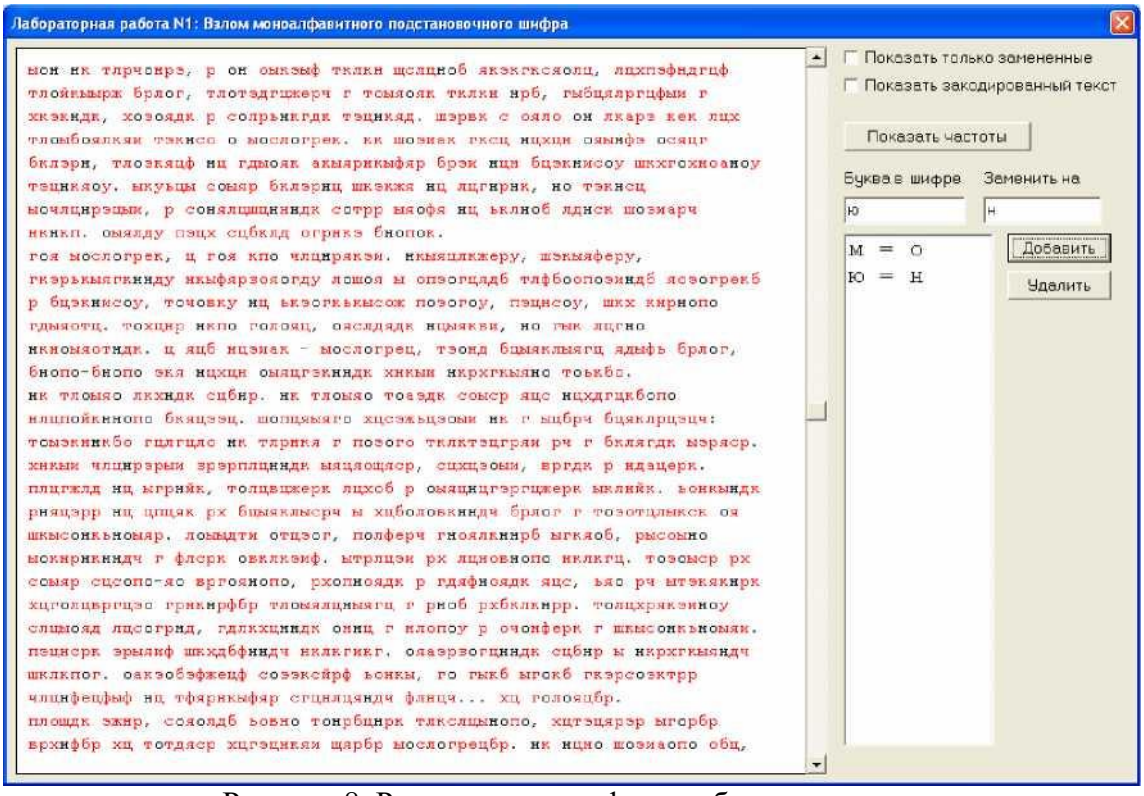


Рисунок 8. Результат расшифровки букв «о» и «н»

Этот фрагмент может быть скорее всего словом « он » В таблице частот (рис. 5) буква «ю» шифра стоит на 5-м месте, что примерно соответствует позиции буквы «н» русского языка (4-е место). Значит разумно попробовать поменять «ю» на «н». Результат приведен на рис. 8.

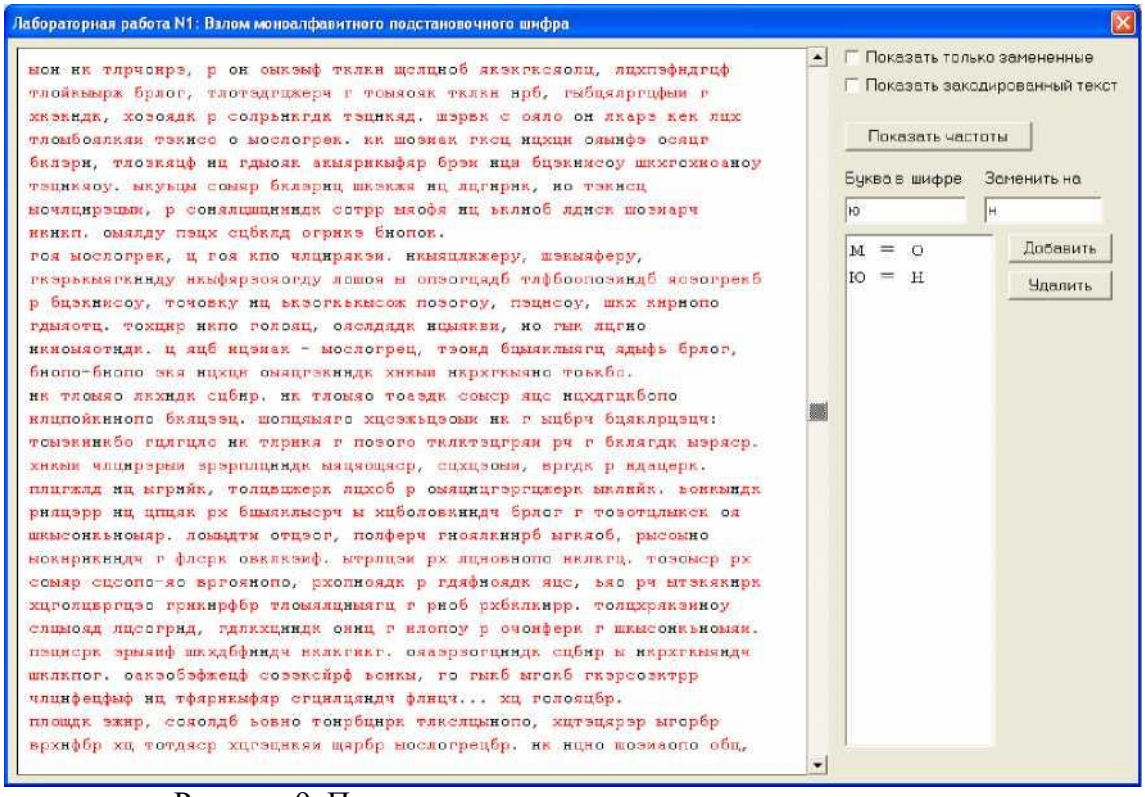


Рисунок 9. Продолжение поиска коротких понятных слов

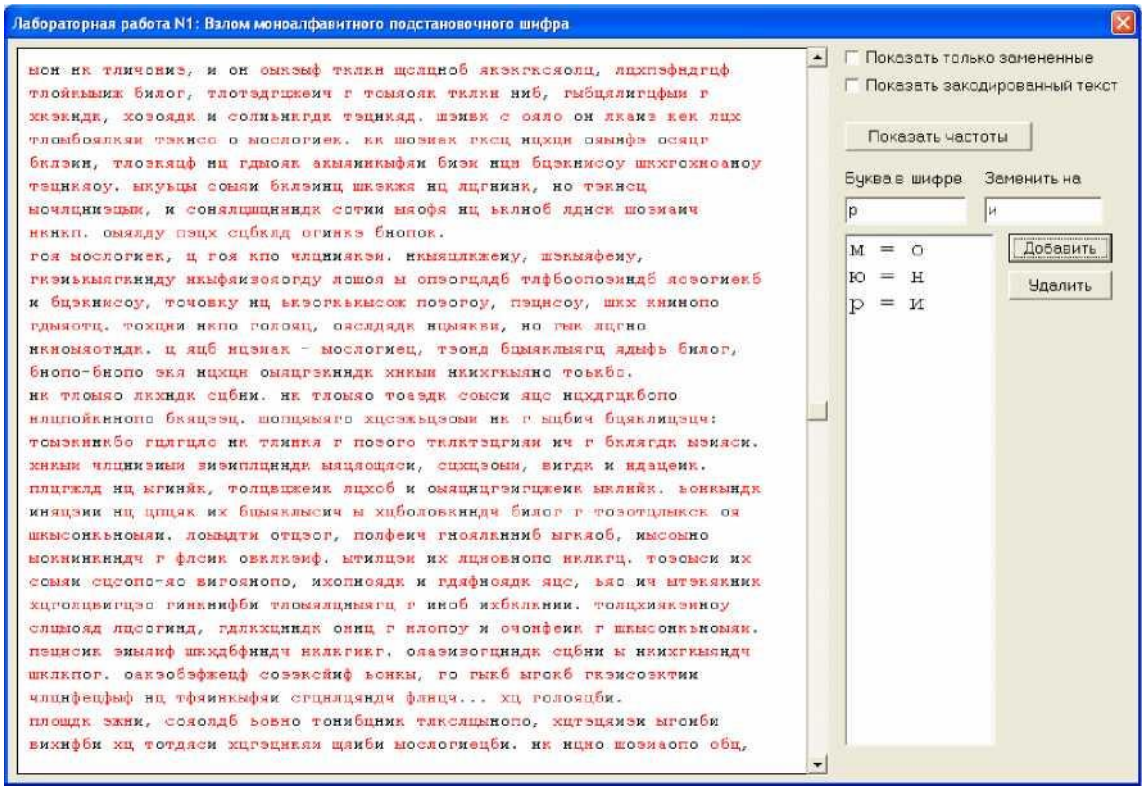


Рис. 10. Результат расшифровки букв «о», «н» и «и»

Далее повторяется поиск коротких слов, в которых можно догадаться о значении зашифрованных букв. На рис. 9 в первой и третей строках есть отдельно стоящее «р». Скорее всего это предлог «и», что согласуется и с информацией на рис. 5. Результат замены приведен на рис. 10.

На рис. 11 в первой строке обнаруживается слово из двух известных «и» и шифрованной буквы «э» между ними. Скорее всего это буква «л», образующая слово «или» (рис. 12).

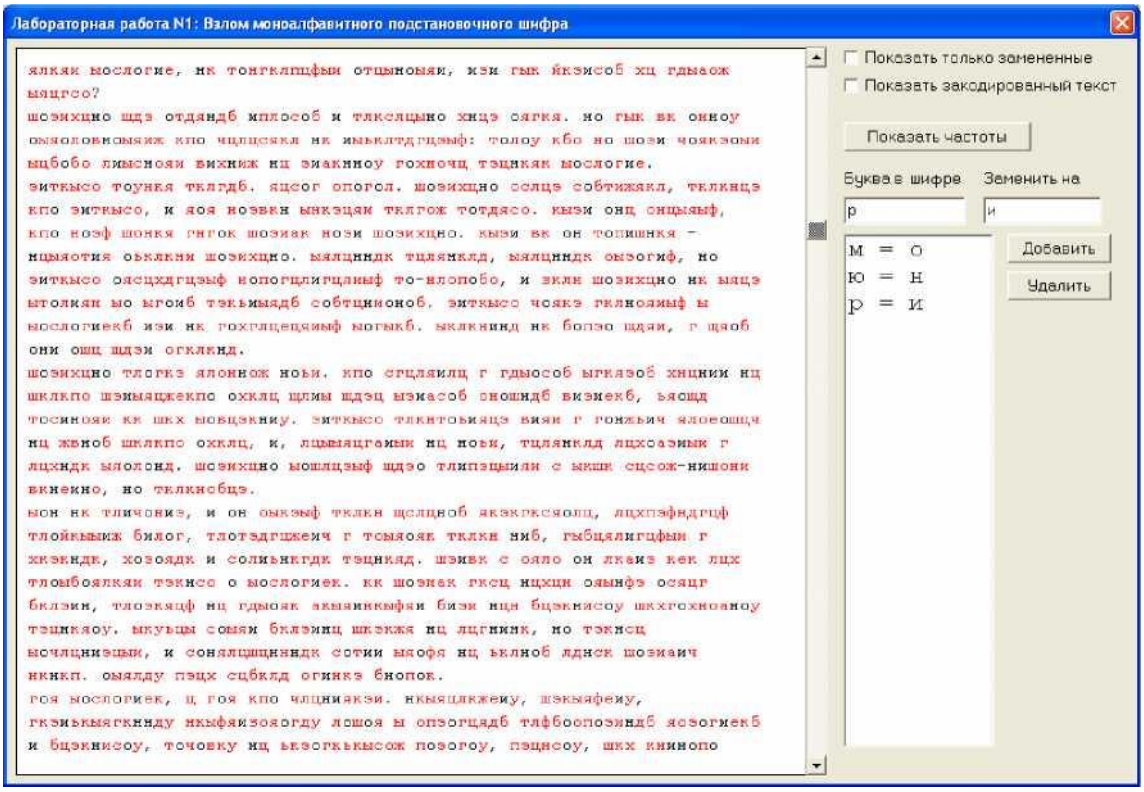


Рисунок 11. Продолжение поиска коротких понятных слов

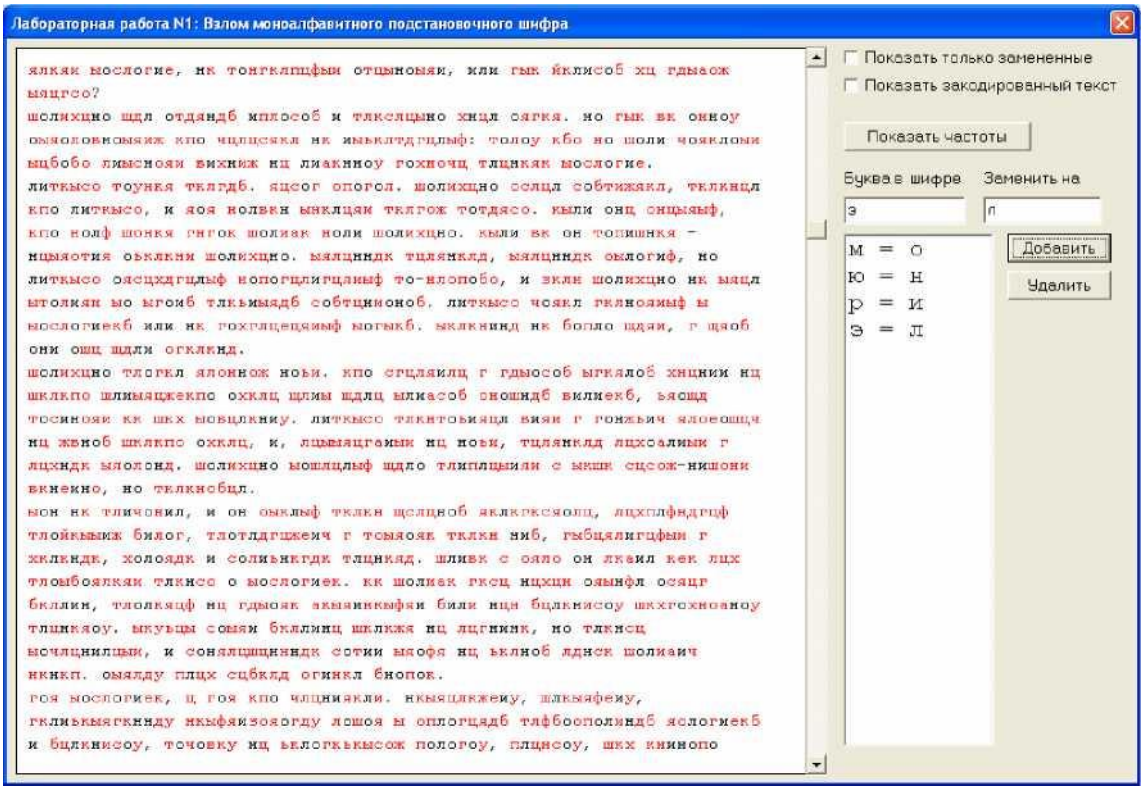


Рисунок 12. Результат расшифровки букв «о», «н», «и» и «л»

После расшифровки аналогичным образом букв «к» на «е», «ц» на «а» и «я» на «т» окно выполнения лабораторной работы приобретает следующий вид (рис. 13):

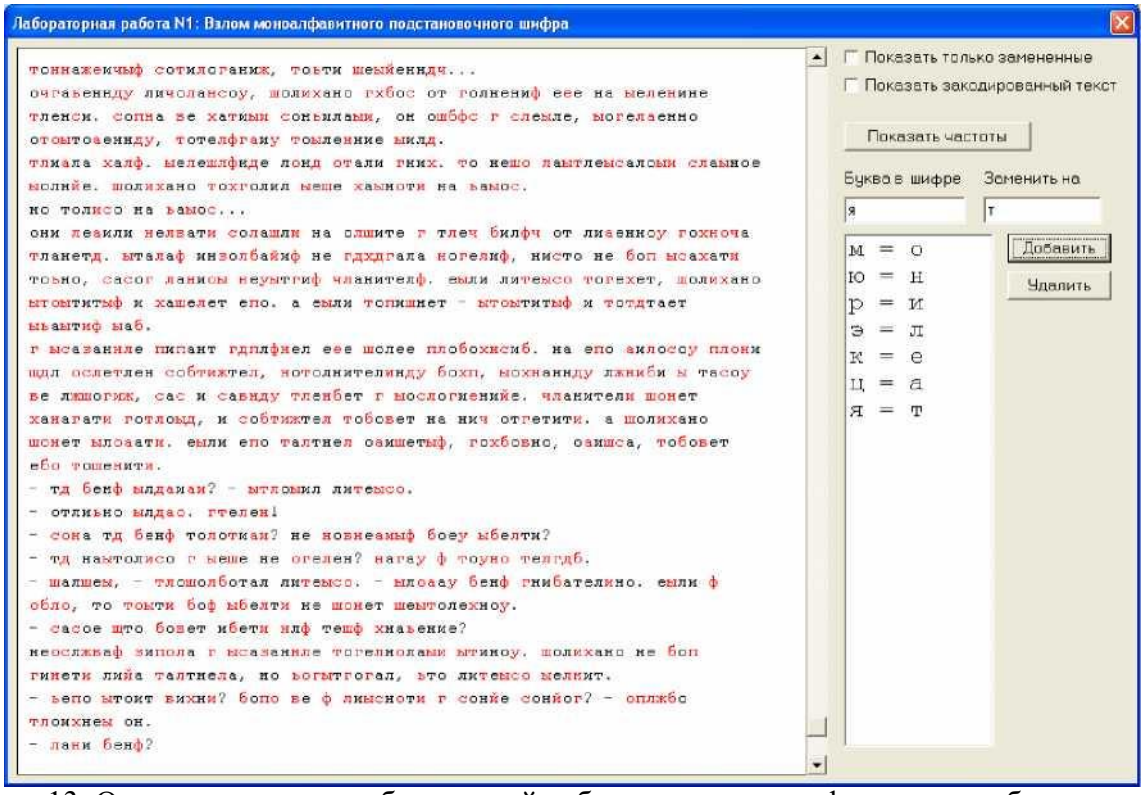


Рисунок 13. Окно выполнения лабораторной работы после расшифровки семи букв

Когда так много букв уже известно, зашифрованные буквы могут мешать для понимания слов. Для облегчения дальнейшего анализа в программе предусмотрена возможность выставления флага «Показать только замененные», при выставлении которого все зашифрованные буквы выводятся на экран в виде символов решетки (рис. 14).

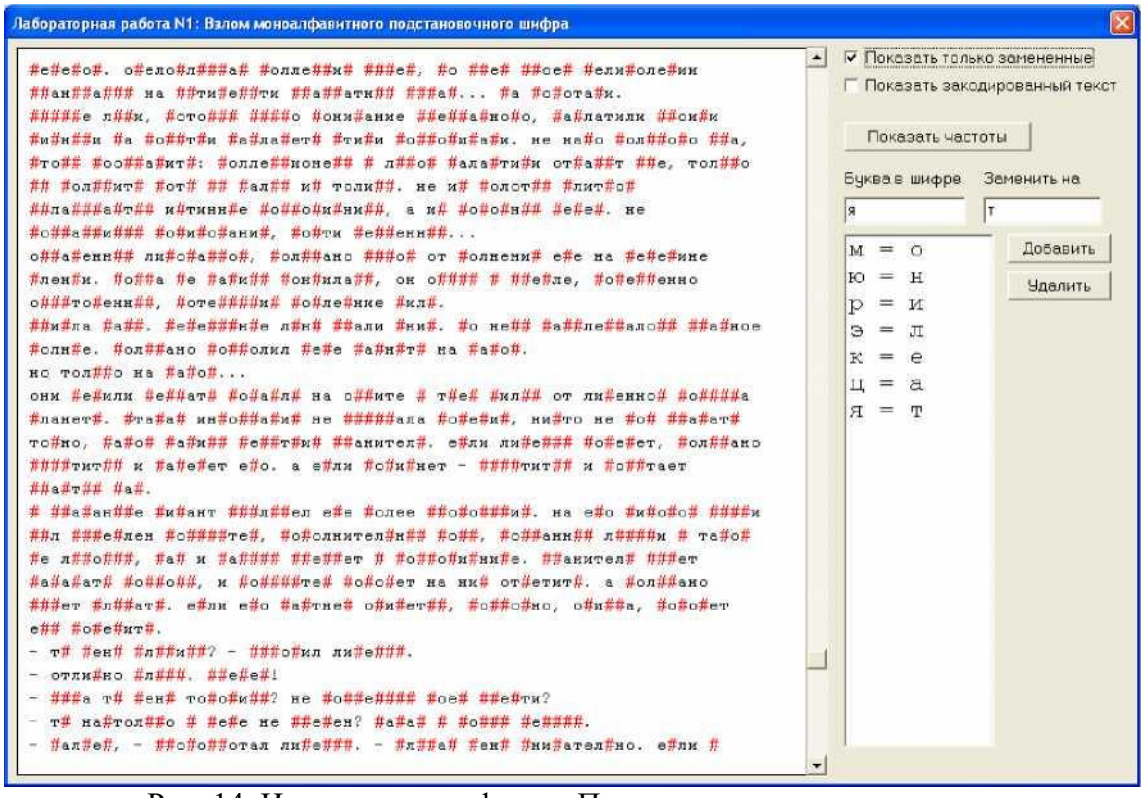


Рис. 14. Использование флага «Показать только замененные»

Теперь видно, что слово «##о#о##отал» в нижней строке вполне может быть словом «пробормотал». Если теперь выключить флаг, то можно получить косвенное подтверждение

этого - на позициях двух букв «р» в этом слове в шифре также находится одинаковая буква «л» (рис. 15).

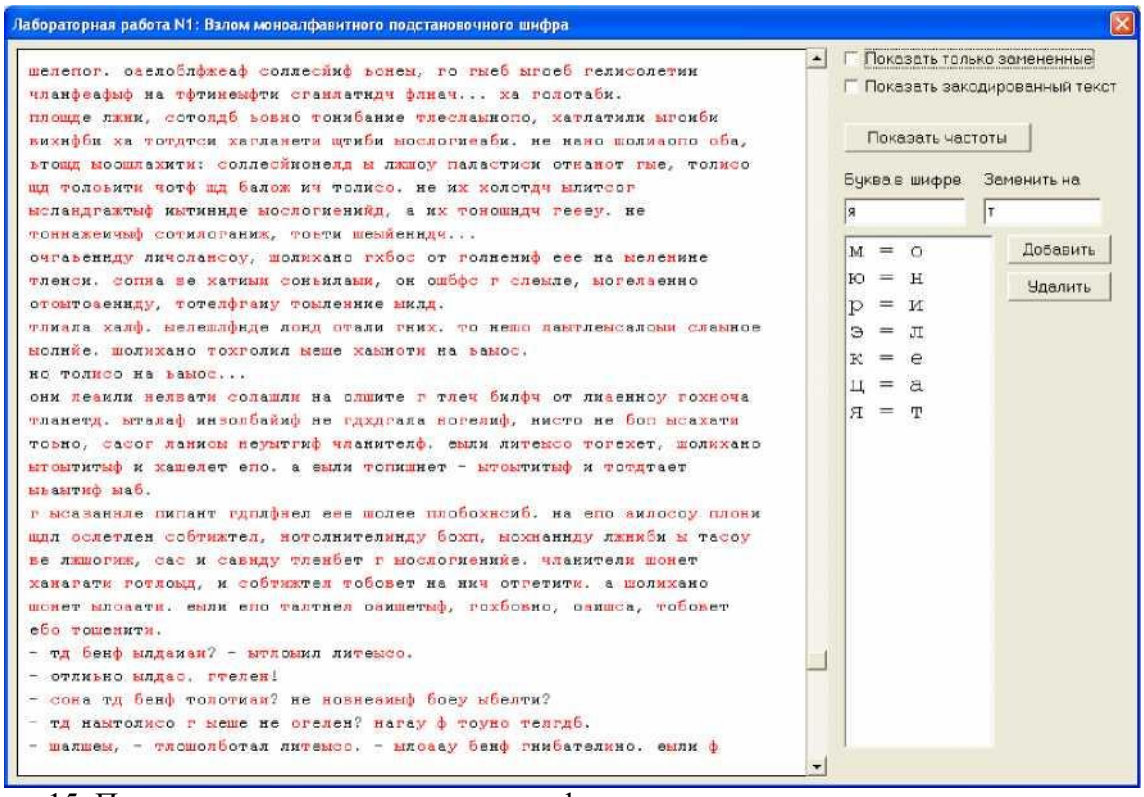


Рисунок 15. Проверка гипотезы отключением флага

Если заменить теперь букву «т» на «п», «л» на «р», «ш» на «б» и «б» на «м», то окно выполнения лабораторной работы станет выглядеть так(рис. 16):

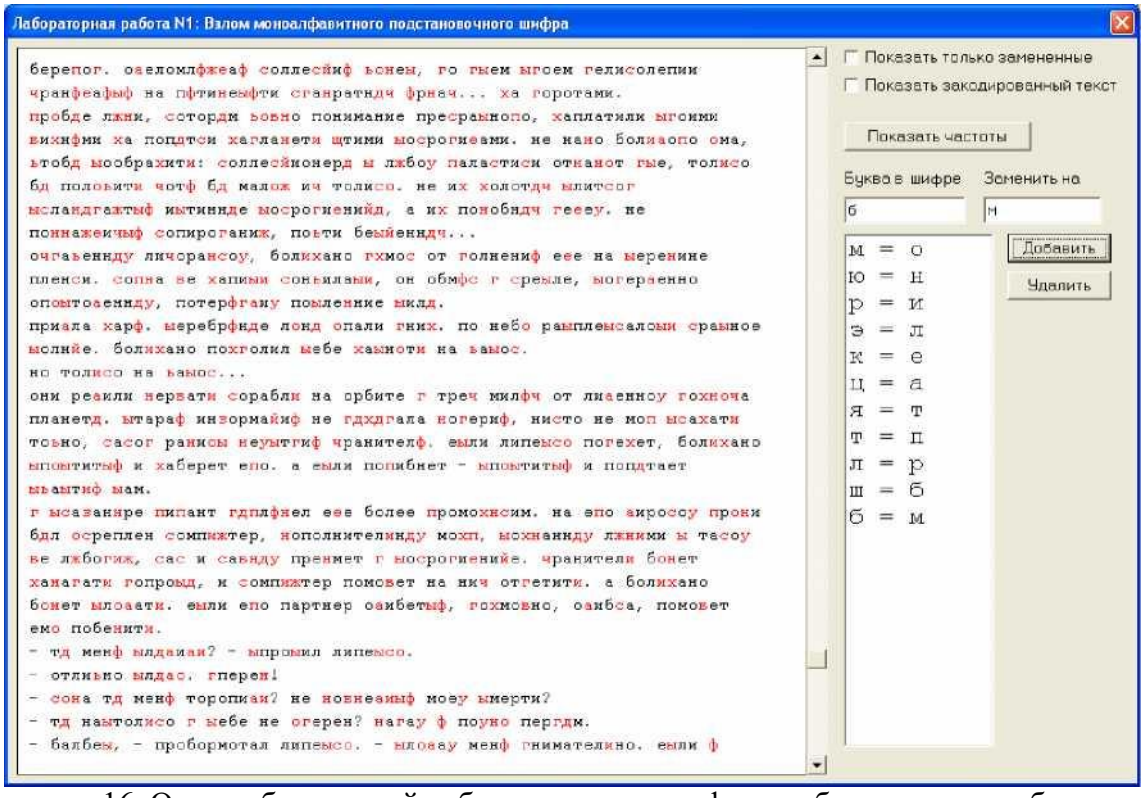


Рисунок 16. Окно лабораторной работы после расшифровки букв «п», «р», «б» и «м».

Хорошо видно, что дальнейший анализ значительно упрощается. Например, очевидно по слову «хаплатили», что буква «х» шифра соответствует букве «з» исходного текста. На рис. 17 приведено окно программы, когда анализ уже близок к завершению (осталось совсем немного нерасшифрованных букв).

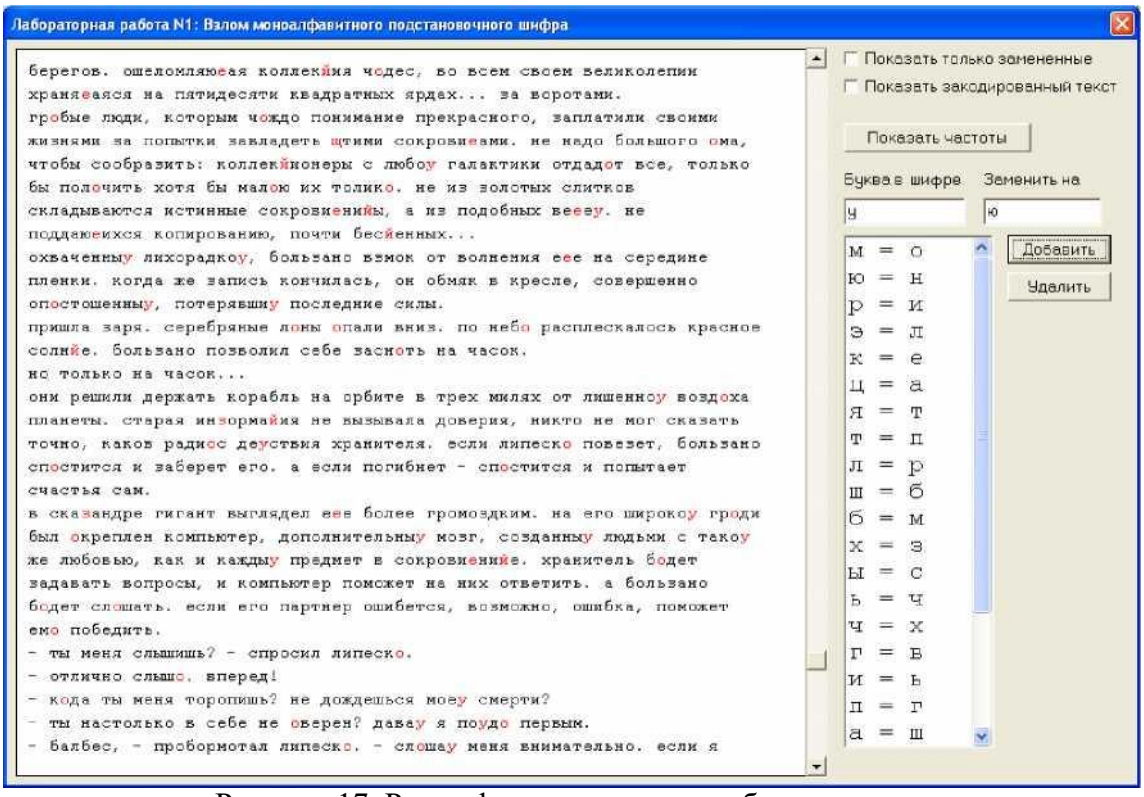


Рисунок 17. Расшифрованы почти все буквы текста

Когда же все буквы текста расшифрованы, на экран выводится информационное окно (рис. 18):

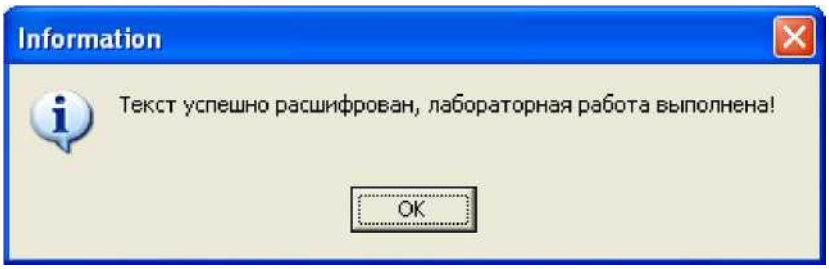


Рис. 18. Информационное окно, свидетельствующее о успешной расшифровке текста

Появление этого окна на экране свидетельствует об успешном выполнении лабораторной работы.

Лабораторная работа 13-14
Одноразовые блокноты

Цель работы. Ознакомиться на практике с принципом действия одноразового блокнота. Используя Matlab, исследовать данную задачу.

Ход выполнения работы.

1. Сгенерируйте одноразовый блокнот (массив случайных чисел), длиной 10 000 000 байт. Используйте для этого функцию rand матлаба.
2. Растяните полученные случайные числа с интервала 0..1 на интервал 0..255.

Переведите числа из формата с плавающей запятой в целочисленный формат. Воспользуйтесь для этого функцией uint8.

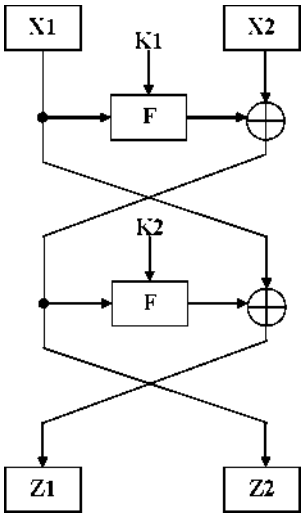
3. Постройте гистограмму распределения значений полученного одноразового блокнота. Воспользуйтесь функцией hist. Постройте гистограмму с 256-ю столбиками. Включите гистограмму в отчет о проведенной работе.
4. Сохраните одноразовый блокнот в файл (используйте функции “fopen”, “fwrite”, “fclose”). Попытайтесь сжать его программой WinRAR или WinZip. Какой коэффициент сжатия был получен? Включите в отчет о проведенной работе точные размеры файла до и после сжатия. Объясните полученные результаты.
5. Создайте переменную типа строка и занесите туда свои ФИО. Например, s=’Пономаренко Николай Николаевич’; Преобразуйте эту строку в целочисленный формат (функция “uint16”). Закодируйте полученный массив сформированным одноразовым блокнотом (используйте функцию bitxor матлаба). Включите в отчет исходную строку, ее целочисленное представление и результат кодирования одноразовым блокнотом. Декодируйте закодированную строку одноразовым блокнотом. Преобразуйте полученный массив обратно в текстовый вид (используйте функцию char матлаба). Выведите результат на экран. Восстановилась ли исходная строка?
6. Добавьте к ФИО еще и номер группы. Например, s=’Пономаренко Николай Николаевич 539’; Закодируйте и декодируйте эту строку аналогично действиям, описанным в пункте 5, но с использованием другого фрагмента одноразового блокнота. Включите полученные результаты в отчет.
7. Предоставьте преподавателю отчет о проделанной работе в электронном или печатном виде, а также текст программы.

Работа должна быть выполнена самостоятельно.

Лабораторная работа №15-16
Сеть Фейштеля

Цель работы. Запрограммировать на языке Матлаб сеть Фейштеля.

1. Напишите на языке Матлаб функцию, вычисляющую выходы сети Фейштеля.



Функция должна иметь вид:
function [z1,z2] = Nikolay(x1,x2,k1,k2,nr)
% здесь должен быть написанный % вами текст программы, который вычисляет % выходы сети Фейштеля
Nikolay - имя функции (придумайте для себя какое-нибудь другое).
На вход функции будут подаваться:
x1, x2 - исходные данные, которые нужно зашифровать (тип данных - uint32) nr - число раундов (повторов) сети Фейштеля
k1, k2 - массивы с материалом ключа (длина каждого из массивов равна r, тип данных - uint32)
На выходе функции должны быть: z1, z2 - выходные зашифрованные данные (тип данных - uint32)
Функция F(x,k):
Число x сдвигается вправо на 3 бита, если раунд - четный, или влево на 2 бита, если нечетный (функция bitshift Матлаба). Результат сдвига складывается суммой по модулю два с k (функция bitxor Матлаба).

2. Напишите на языке Матлаб функцию, которая декодирует ранее закодированные данные z1 и z2.
Чтобы декодировать один раунд сети Фейштеля (последний раунд r), запишем выражения для z1 и z2. z1 = x1 xor F(z2, k2(nr)) z2 = x2 xor F(x1 , k1 (nr))
Отсюда можно найти сначала x1 (здесь xor - сумма по модулю два): x1 = z1 xor F(z2, k2(nr))
а потом и x2:
x2 = z2 xor F(x1 , k1 (nr))
Это действие должно повторяться в цикле nr раз.
Пример цикла, который идет в обратном порядке и выводит на экран числа от nr до 1:

```
for  kkk=nr:-
1:1
disp(kkk);
```

3. Попробуйте проверить работоспособность ваших двух функций. Предоставьте преподавателю для проверки тексты программ в электронном виде.

Лабораторная работа №17-18
Шифрование с открытым ключом и электронная цифровая подпись на GPG

Цель работы. Ознакомиться с программой GPG (Kleopatra), научиться генерировать с ее помощью открытый и закрытый ключи, подписывать файлы и проверять подпись, шифровать и расшифровывать файлы, передавать другим пользователям свой открытый ключ.

1. Ознакомьтесь с историей создания программы PGP (http://ru.wikipedia.org/wiki/PGP).
2. Из папки лабораторной работы установите программу gpg4win-2.1.0.exe. Устанавливать только те части программ, которые предлагается устанавливать по умолчанию.
3. Запустите программу Kleopatra. Сгенерируйте пару открытого и закрытого ключа, используя для этого пункт меню “New Cerificate” (рис. 1).

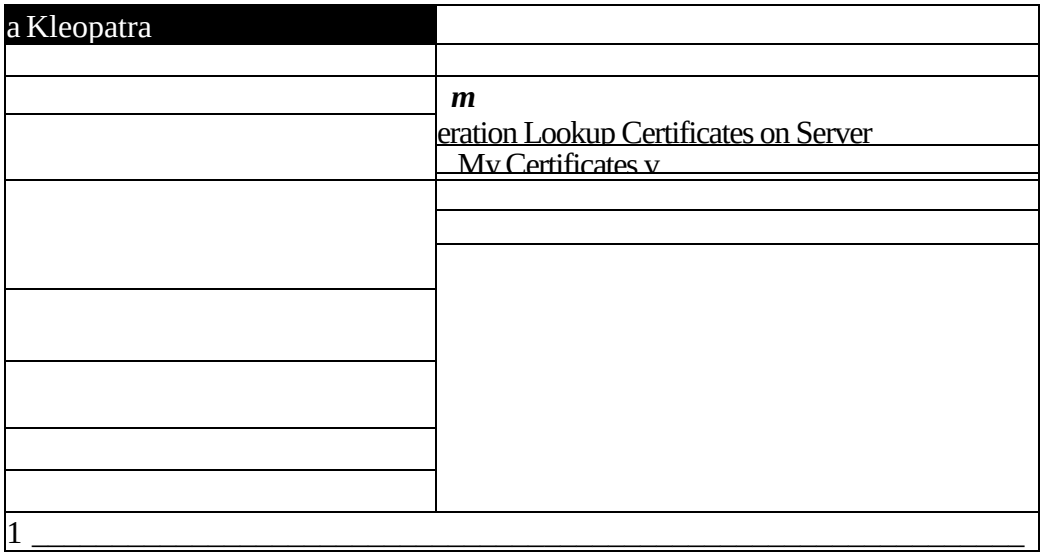


Рис. 1. Окно программы Kleopatra

При этом выберите опцию “Create a personal Open PGP key pair” и в появившемся окне (рис. 2) введите свои данные (имя и e-mail).

Рис. 2. Окно ввода параметров

Нажмите кнопочку “Advanced Settings” и выберите ключ RSA 3072 бит.

4. После генерации ключа программа запросит пароль (этот пароль нужен, чтобы никто, кроме Вас не мог использовать Ваш закрытый ключ даже, если похитит Ваш компьютер со сгенерированной парой ключей. Также Вам предложат сохранить пару ключей в файл. Сохраните их.
5. Экспортируйте ключ в текстовый файл (для будущей передачи друзьям и знакомым). Для этого воспользуйтесь пунктом “Export Certificates” меню ”File”. Передайте этот файл преподавателю (копируйте его и последующие файлы в папку со своей фамилией в директорию user_files в папке с лабораторной работой).
6. Импортируйте открытый ключ преподавателя “ponom.asc”, воспользовавшись пунктом “Import Certificates” меню ”File”.
7. Сформируйте текстовое сообщение. Зашифруйте это сообщение ключом преподавателя (пункт “Sign/Encrypt Files” меню ”File”. Попытайтесь расшифровать зашифрованный файл. Передайте зашифрованный файл преподавателю.
8. Сформировать второе текстовое сообщение. Подписать его своим ключом. Передать текстовое сообщение и цифровую подпись преподавателю.
9. Сформировать третье текстовое сообщение. Зашифровать его открытым ключом преподавателя и сохранить результат в текстовом виде (опция в программе). Подписать зашифрованное сообщение своей подписью и передать полученные файлы преподавателю.

Лабораторная работа № 19-20
Метод шифрования с открытым ключом RSA

Цель работы. Ознакомиться на практике с методом шифрования RSA и особенностями его практической реализации (возведение больших чисел в большие степени с использованием модулярного умножения по Монтгомери и метода двоичного возведения в степень).
Исходные данные:
Зашифрованное число C, закрытый ключ D, часть открытого ключа N.
Выходные данные:
Нужно декодировать число M .
Теоретические основы:

Для расшифровки числа M в методе RSA до статочно зашифрованное число C возвести в степень D и найти остаток от деления на N.

Основная проблема, возникающая при практическом использовании метода RSA, заключается в том, что числа C, D и N являются очень большими. Использовать традиционные методы умножения чисел при возведении числа C в степень D не получится из-за переполнения вычислительного устройства. На практике используют метод бинарного возведения в степень для сокращения количества умножений, а также метод модулярного умножения по Монтгомери для того, чтобы не выходить из разрядности чисел C, D и N в процессе умножения больше, чем на 1 разряд.
Методические указания:
1. Воспользуйтесь двоичным методом возведения в степень, чтобы определить последовательность умножений (текущий результат умножается сам на себя или же на исходное число), которая минимизирует общее число операций умножения.
2. Переведите число C в модулярную форму.
3. Возведите C в степень D двоичным методом, пользуясь модулярным умножением по Монтгомери (используйте на исходное число C, а его модулярную форму!).
4. Переведите число из модулярной формы в обычную. Для этого умножьте его на 1по Монтгомери.
5. Проверьте расшифрованное сообщение M (введя его в строку «Декодированное сообщение» и нажав кнопку «Проверить»).
Окно программы выполнения лабораторной работы:

Эта программа представляет собой калькулятор, в котором реализованы все необходимые для выполнения лабораторной работы функции: перевод из обычной формы в модулярную, перевод числа из десятичной системы счисления в двоичную, а также умножение по Монтгомери.

На рис. 1 приведено окно программы.

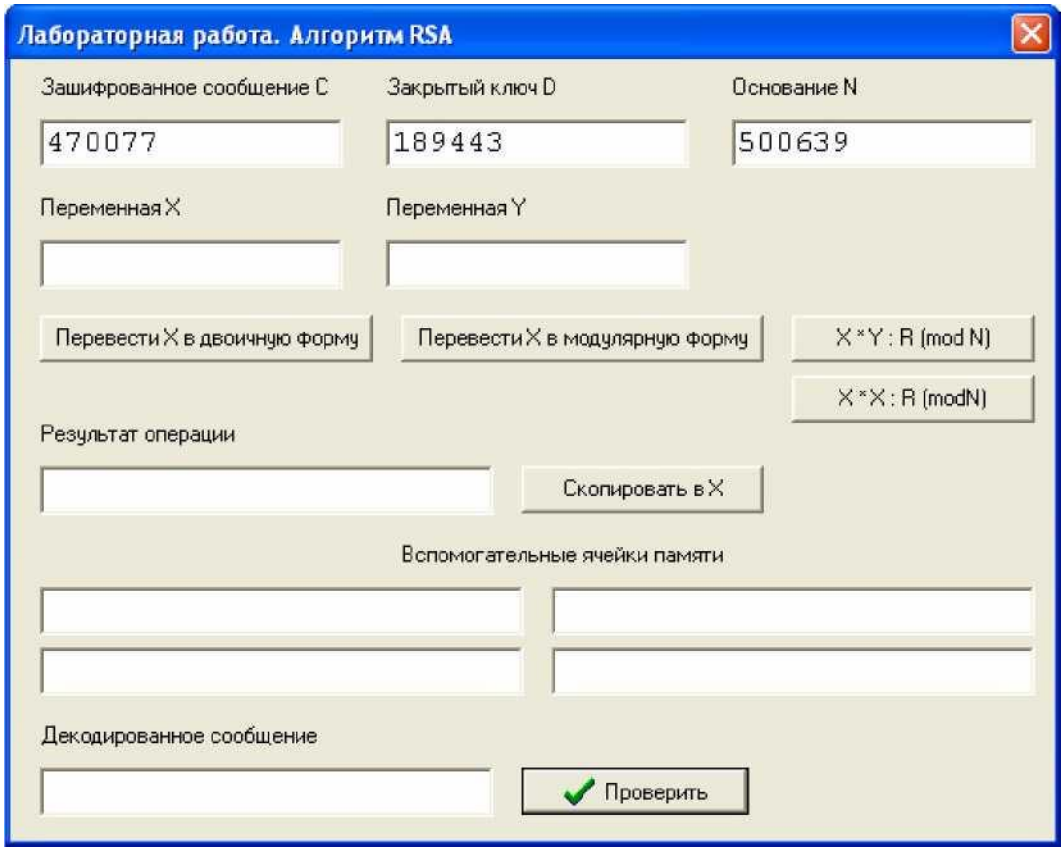


Рис. 1. Окно программы выполнения лабораторной работы

В верхних трех строках ввода находятся исходные данные для выполнения работы. Содержимое любой строки ввода в данной программе можно выделить и скопировать (правая клавиша мыши или же комбинация клавиш “Ctrl-C”) и вставить в другую строку ввода (правая клавиша мыши или же комбинация клавиш “Ctrl-V”).

Копка “Перевести X в двоичную форму” переводит содержимое строки ввода “Переменная X” в двоичный вид и помещает результат в строку ввода “Результат операции”.

Кнопка “Перевести X в модулярную форму” переводит содержимое строки ввода “Переменная X” в модулярную форму и помещает результат в строку ввода “Результат операции”.

Кнопка “X*X : R (mod N)” выполняет умножение по Монтгомери содержимого строки ввода “Переменная X” само на себя и помещает результат в строку ввода “Результат операции”.

Кнопка “X*Y : R (mod N)” выполняет умножение по Монтгомери содержимого строки ввода “Переменная X” на содержимое строки ввода “Переменная Y” и помещает результат в строку ввода “Результат операции”.

Кнопка “Скопировать в X” помещает результат последнего вычисления (содержимое строки ввода “Результат операции”) в строку ввода “Переменная X”.

Четыре строки ввода, располагающиеся ниже, являются вспомогательными и погут использоваться для хранения любой информации, например, числа D в двоичном виде.

Копка “Проверить” предназначена для проверки правильности полученного результата, который должен быть предварительно помещен в строку ввода “Декодированное сообщение”.

Лабораторная работа №21-22

Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.

Цель работы. Ознакомиться на практике с работой хэш-функций. Написать на Matlab программу для оценивания устойчивости пароля ко взлому.

Теоретические основы:

Оценим устойчивость U пароля по взлому.

1. Пусть L - длина пароля.
   Если длина пароля L < 4, то U=0
   иначе, если 5 < L < 7, то U=6
   иначе, если 8 < L < 15, то U=12
   иначе, если 16 < L, то U=18
2. Если в пароле есть буквы, но только в одном (нижнем или верхнем регистре), то U=U+5
   иначе, если в пароле есть буквы и в нижнем и в верхнем регистрах, то U=U+7
3. Пусть N - число цифр в пароле.
   Если число цифр в пароле 1 < N < 2, то
   U=U+5 иначе, если 3 < N, то U=U+7
4. Пусть S - число спецсимволов (#$%@) в в пароле.
   Если 1 < S < 2, то U=U+5
   иначе, если 2 < S, то U=U+10.
5. Если в пароле есть буквы в обоих регистрах, спецсимволы и цифры, то
   U=U+6 иначе, если только чего-то одного из этого нет, U=U+4.

Если U < 16 . пароль очень слабый
иначе, если 15 < U < 25 - слабый
иначе, если 24< U < 35 - средний
иначе, если 34< U < 45 - сильный
иначе, если 44 < U - очень сильный

Методические указания:

1. Создайте на своем компьютере какой-нибудь рабочий подкаталог и скопируйте туда *.m файлы из каталога лабораторной работы. Запустите Matlab и выберите созданный подкаталог в качестве “Current Directory”.
2. Ознакомьтесь с прилагаемой к лабораторной работе функцией вычисления хэш-функции MD5 (файл md5.m). Наберите в Matlab команду help md5
3. Присвойте текстовой переменной свое ФИО. Например, Б=’Пономаренко Николай Николаевич’; Вычислите значение MD5 для этой переменной. Измените какую-нибудь одну букву в своем ФИО. Вычислите значение MD5 для измененного текста. Поясните полученный результат.
4. Поясните, как хэш-функция может использоваться при аутентификации для того, чтобы обеспечить подлинность сеанса связи и скрыть пароль, передаваемый по каналам связи от пользователя к серверу.
5. Напишите программу для оценивания сложности пароля (заданного в виде текстовой строки). В подкаталоге лабораторной работы выложены функции, облегчающие написание этой программы:

isbigl(s) - возвращает 1, если s - буква в верхнем регистре issml(s) - возвращает 1, если s - буква в нижнем регистре iscif(s) - возвращает 1, если s - цифра isspec(s) - возвращает 1, если s - спецсимвол

Ознакомьтесь с текстами этих функций и используйте их при написании своей программы.

6. Продемонстрируйте на примерах работу своей программы. Приведите примеры среднего и сильного паролей.

Лабораторная работа № 23-25

Тема: Исследование основных характеристик сигналов на основе использования аппаратно-программного комплекса радиоконтроля «КВАДРАТ»

Цель работы:

- Изучить основные элементы и их назначение основного окна программы RT2060 (см. приложение).

Порядок выполнения работы

- ознакомится с представленным материалом;
- ознакомится с программой RT2060_Demo;
- ответить на контрольные вопросы;
- оформить отчет.

1. Основное окно программы

Основное окно программы (рис 3.1) содержит: 1) экран спектральных панорам; 2) экран спектрограммы; 3) экран отображения спектров обнаруженных сигналов; 4) список обнаруженных сигналов; 5) зону индикации параметров управления (внизу);

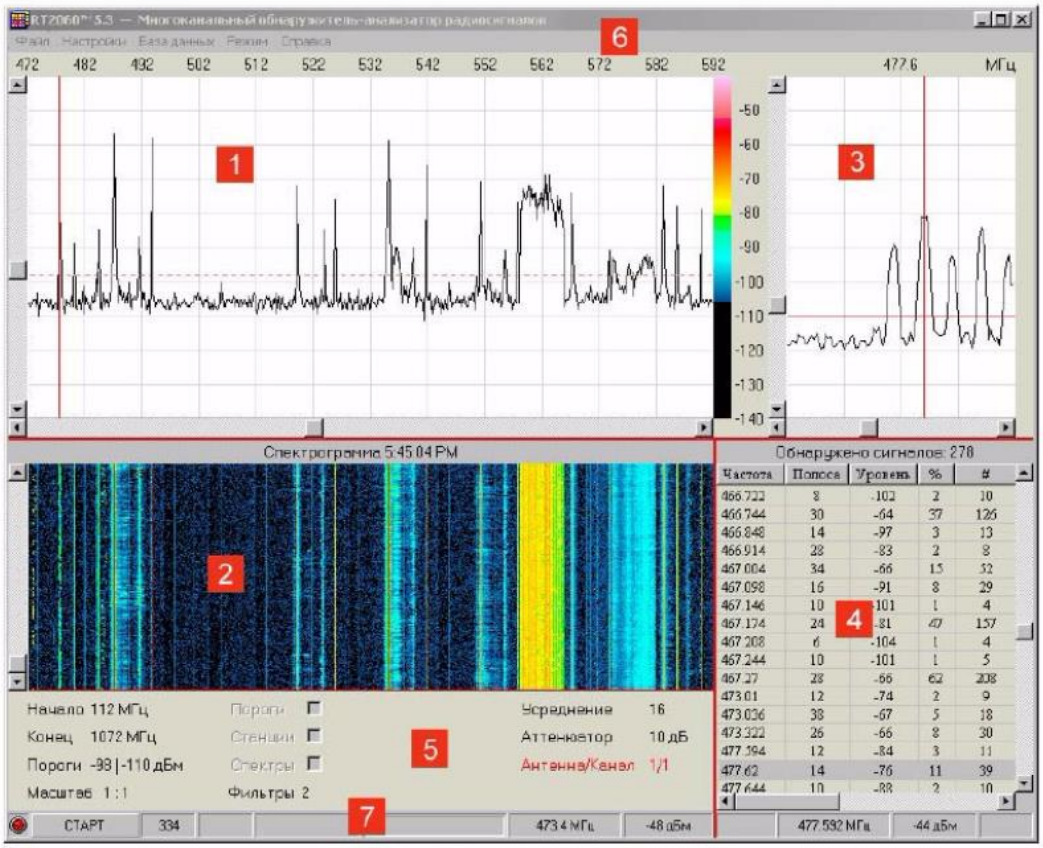


Рис. 3.1. Основное окно программы RT2060

6) строки названия и меню в верхней части основного окна; 7) строку сообщений о состоянии программы и параметрах сигнала в нижней части основного окна программы, где находятся также кнопка запуска/остановки режима сбора данных и индикатор процесса обзора.

Оператор может выбрать удобный для отображения всех элементов размер окна. Для этого курсор мыши наводится на нужную границу окна, после чего форма курсора должна измениться. Затем граница может перемещаться мышью при нажатой левой кнопке.

Размеры панелей, в которых находятся экран спектральных панорам, спектрограмма и список обнаруженных сигналов, могут изменяться с помощью мыши. Границы этих панелей выделены красными

линиями. Если навести на одну из таких линий курсор мыши, он изменит свой вид и позволит перемещать границу, не отпуская левую кнопку мыши. Изменение границ панелей дает возможность, например, расширить видимую часть списка обнаруженных сигналов при анализе данных радионаблюдения.

2. Экран спектральных панорам.

Экран размером 600 (ширина) на 300 (высота) элементов изображения (рис. 3.1,
позиция 1) разделен линиями разметки на 12 и 10 делений соответственно по горизонтали и вертикали. Лини разметки находятся на заднем плане относительно отображаемых реализаций спектра. На этом экране данные радионаблюдения отображаются в виде панорам спектров в координатах уровень-частота. Уровень сигнала измеряется на антенном входе в децибелах относительно одного милливатта (дБм) без учета ослабления в аттенюаторе приемника. Цена деления вертикальной шкалы- 10 дБ, верхней линии соответствует уровень —40 дБм. Полоса анализа (разрешение) составляет 200 кГц. В зависимости от выбранного масштаба отображения цена деления горизонтальной оси составляет 10, 5 или 2 МГц.
При этом на экран выводится полоса частот 120, 60 или 24 МГц. Масштаб отображения меняется двойным щелчком мыши по надписи Масштаб в нижней части основного окна.

В нижней части экрана находится полоса прокрутки по горизонтальной (частотной) оси, помощью которой можно выбирать для просмотра нужный участок спектральной панорамы, если вся полоса обзора не умещается на экране. Щелчок мыши по полосе прокрутки слева или справа от движка вызывает сдвиг панорамы на ширину одного окна (120, 60 или 24 МГц в зависимости от масштаба отображения). Щелчок мыши по левой или правой стрелкам полосы прокрутки сдвигает панораму на 10, 5 или 2 МГц в зависимости от выбранного масштаба отображения. Сдвигать панораму по частотной оси можно также буксировкой движка полосы прокрутки при нажатой кнопке мыши, В режиме сбора данных команды на сдвиг панорамы по частотной оси могут выполняться с задержкой в несколько
секунд.

Левая полоса прокрутки используется для установки базового порога обнаружения, который отображается на экране штриховой линией (см. раздел 6 Редактор пороговых уровней) и выводится в числовом виде в левой части области отображения параметров (позиция 5). В правой части окна находится цветовая полоса, которая используется для индикации уровней и установки цветового порога спектрограммы (см. раздел 2).

Щелчок левой кнопки мыши по экрану спектральных панорам вызывает появление вертикальной маркерной линии. Одновременно на частоту этой линии настраивается экран отображения спектров обнаруженных сигналов, центр которого также отмечается маркерной линией. Для измерения уровней и частот сигналов на спектральной панораме используется курсор мыши, координаты которого (частота в МГц, уровень в дБм) выводятся в строке состояния программы в позициях 7 и 8 (см. раздел 8 Строка отображения состояния программы). Пользователь может изменять оформление экрана (цвета и яркости фона, реализаций сигналов, курсоров и линий разметки) в закладке Вид панели Настройки, которое вызывается командой меню Настройки (см. раздел 4 Настройка внешнего вида).

3. Экран спектрограммы.

На этом экране (рис. 3.1, позиция 2) данные радионаблюдения показываются в виде спектрограммы, которая отражает изменение спектральной панорамы во времени. Горизонтальная ось соответствует оси частот, вертикальная — времени, а уровни спектра отображаются цветовой кодировкой. Масштаб отображения по оси частот соответствует масштабу экрана спектральных панорам. В зависимости от выбранного масштаба отображения цена деления горизонтальной оси составляет 10, 5 или 2 МГц. При этом на экран выводится полоса частот 120, 60 или 24 МГц. Масштаб отображения меняется двойным щелчком мыши по надписи Масштаб в нижней части основного окна.

Каждая текущая панорама спектра записывается в буферную память емкостью
200 реализаций и отображается в виде горизонтальной линии на частотно временной плоскости, причем изменение уровней от больших к меньшим передается цветом в соответствии с выбранной цветовой таблицей. По умолчанию программа использует цветовую таблицу индексированных цветов (256 градаций) с близким к естественному порядком изменения цвета от черного (слабые сигналы) к красному (сильные сигналы). Соответствие уровней сигнала цветам спектрограммы устанавливает цветовая полоса в правой части окна спектральных панорам. Если навести курсор мыши на выбранный цвет, появится указатель соответствующего значения мощности в дБм. Все уровни внизу цветовой полосы отображаются одним (черным) цветом. Изменить положение границы черной области можно щелчком мыши. О настройке цветовой таблицы см. раздел 3.2.4 Настройка внешнего вида.

После заполнения буферная память начинает работать в стековом режиме, когда запись каждой новой реализации вызывает сдвиг стека и стирание самой старой реализации. Линии текущих спектров последовательно заполняют спектрограмму снизу вверх, причем вновь зарегистрированные реализации находятся внизу, а зарегистрированные ранее располагаются выше.

После остановки режима сбора данных щелчком мыши по экрану спектрограммы можно выбрать нужную панораму для просмотра в окне спектральных панорам. При этом на этом экране спектрограммы появится горизонтальная маркерная линия, соответствующая ей панорама будет отображаться в экране спектральных панорам, а в заголовке экрана спектрограммы справа от надписи Спектрограмма будет отображаться время регистрации этой панорамы. Кроме того, изменится значение счетчика числа циклов обзора, расположенного в строке состояния программы в позиции 3 (см. раздел 8 Строка отображения состояния программы). Слева от экрана спектрограммы находится полоса прокрутки по вертикальной (временной) оси. Щелчок мыши по верхней или нижней стрелке полосы прокрутки вызывает переход соответственно к более поздней или ранней спектральной панораме, щелчок мыши выше или ниже движка полосы прокрутки вызывает переход во времени на 10 циклов сканирования вперед или назад. Изменять положение горизонтального маркера можно также буксировкой движка полосы прокрутки при нажатой кнопке мыши.

Щелчок мыши по цветовой полосе в правой части окна спектральных панорам вызывает изменение черной области цветовой полосы и, следовательно, цветового порога. При этом следы всех сигналов, уровни которых меньше выбранного порогового значения, на спектрограмме не отображаются, поскольку сливаются с фоновым черным цветом. Изменение цветового порога используется при исследовании спектрограмм в качестве средства селекции сигналов по уровню.

4. Экран отображения спектра.

На этом экране (рис. 3.1, позиция 3) отображаются спектры обнаруженных сигналов из базы данных программы, зарегистрированные в каждой из антенн комплекса. Уровень сигнала измеряется на антенном входе в децибелах относительно одного милливатта (дБм). Цена деления вертикальной шкалы — 10 дБ, верхней линии соответствует уровень —40 дБм. Полоса анализа (разрешение) составляет 2 кГц. Полоса обзора экрана равна 200 кГц, центральная частота отображается в верхней части экрана. Цена деления горизонтальной шкалы - 50 кГц. Лини разметки находятся на заднем плане относительно отображаемых реализаций спектра. для просмотра спектров в различных антеннах необходимо дважды щелкнуть мышью по надписи Антенна/Канал в области отображения параметров основного окна программы или воспользоваться клавиатурной комбинацией <CTRL + C>. Левая полоса прокрутки используется для установки базового порога различения, который отображается на экране сплошной горизонтальной линией (см. раздел 5 Редактор пороговых уровней) и выводится в числовом виде в нижней части экрана. Внизу экрана находится полоса горизонтальной прокрутки, с помощью которой можно изменять центральную частоту экрана и просматривать спектры хранимых в базе данных сигналов. Щелчок мыши по правой или левой стрелке полосы прокрутки изменяет центральную частоту экрана на 200 кГц соответственно в сторону увеличения и уменьшения. Щелчок мыши по полосе прокрутки слева или справа отдвижка вызывает изменение центральной частоты на 1 МГц. Изменить центральную частоту экрана можно также буксировкой движка полосы прокрутки при нажатой кнопке мыши. Одновременно с изменением центральной частоты экрана смещается частотный маркер на экране спектральной панорамы. Если экран отображения спектра на некоторой частоте окажется пустым, то в базе данных сигналы в этом 200-кГц отрезке диапазона отсутствуют. В режиме сбора данных команда изменения центральной частоты экрана выполняется только после завершения цикла обзора.

Для измерения уровней и частот сигналов и их спектральных составляющих используется курсор мыши, координаты которого (частота в МГц, уровень в дБм) выводятся в строке состояния программы в позициях 10 и 11 справа от координат измерительного курсора экрана спектральной панорамы (см. раздел 8 Строка отображения состояния программы).

5. Список обнаруженных сигналов.

Список (рис. 3.1, позиция 4) представляет собой результат запроса к базе данных (отчет). Каждая строка списка содержит параметры обнаруженного сигнала. В верхней строке содержатся заголовки столбцов списка для записи определенных параметров. В столбец Частота записывается несущая частота сигнала в МГц. В столбец Полоса - ширина спектра по уровню порога различения в кГц. Абсолютное значение мощности сигнала в полосе, равной ширине спектра, на антенном входе в дБм записывается в столбец Уровень. Значок % отмечает столбец регулярности или частоты обнаружений (отношение числа

обнаружений сигнала к общему числу циклов обзора за все время наблюдений) в процентах. Значок #- столбец абсолютного числа обнаружений сигнала за все время наблюдений. В
столбце со значком = находится коэффициент совпадения формы спектра сигнала с эталонным спектром. Столбец со значком <A> выделен для отображения отношения уровней сигнала (в дБ) в разнесенных антеннах, столбец, отмеченный значком .- для указания номера антенны (канала), в котором уровень сигнала максимальный. Последние два столбца выделены для даты/времени первого обнаружения сигнала и текстовых примечаний. Список заполняется после обработки данных радионаблюдения. Программа заносит в него только те сигналы, которые отвечают классификационным признакам, установленным при настройке (см.раздел 6 Настройка запроса к базе данных). Видимый размер списка можно изменить буксировкой мышью его границ, выделенных красным цветом. Если список не умещается в видимой части окна, возникают полосы прокрутки, с помощью которых можно просмотреть все записи. Границы столбцов списка можно изменять мышью, если навести ее курсор на границу между столбцами в заголовке. После того как курсор изменит форму, граница передвигается при нажатой левой кнопке мыши. В заголовке списка выводится информация о режиме работы программы и число обнаруженных сигналов, удовлетворяющих классификационным признакам.

Список может быть упорядочен по возрастанию или убыванию любого параметра
щелчком мыши по заголовку его столбца (кроме столбца примечаний). По умолчанию список упорядочен по возрастанию несущей частоты, для вызова спектра обнаруженного сигнала из базы данных необходимо выделить мышью его запись в списке. Спектр появится на правом экране, а несущая частота сигнала отмечается вертикальной маркерной линией. Одновременно на частоте выбранного сигнала появится маркерная линия на экране спектральных панорам. Просматривать спектры сигналов из списка удобно с помощью клавиш <стрелка вверх> и <стрелка вниз> клавиатуры компьютера. Выделить несколько сигналов для удаления из базы данных можно с помощью мыши, одновременно нажимая клавиши <CTRL> или <SHIFT>. При этом группа выделенных сигналов дополнится соответственно одним выделенным сигналом или всеми сигналами от первого выделенного до последнего.

6. Индикация параметров управления.

В зоне отображения параметров управления программой (рис. 3.2) выводится текущая информация о параметрах настройки. В левой колонке отображается начальная и конечная частоты полосы обзора. Двойной щелчок мыши в этой области вызывает закладку Панорама панели Настройки, где можно изменить значения этих параметров. Ниже отображаются пороги обнаружения/различения, которые устанавливаются полосами вертикальной прокрутки соответственно экранов спектральных панорам и спектров обнаруженных сигналов. двойной щелчок мыши по надписи Масштаб вызывает изменение масштаба изображения на экране спектральных панорам.

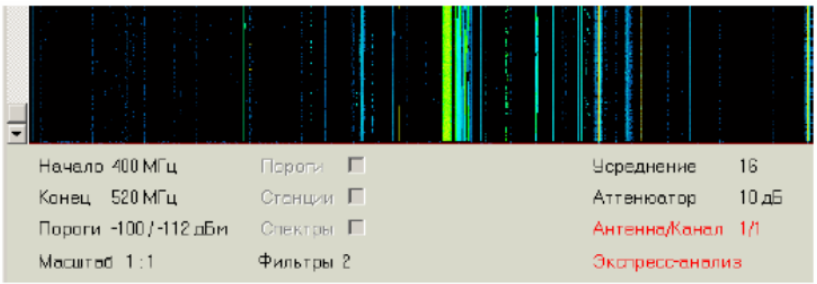


Рис. 3.2. Область индикации параметров управления программой RT2060 располагается под экраном спектрограммы

В средней колонке справа от надписи Пороги выводится имя загруженного файла
порогов. Там же находится позиция, которая помечается галочкой, если пороговую схему этого файла необходимо использовать (см. раздел 5). Двойной щелчок мыши по имени файла вызывает закладку Пороги панели Настройки, где этот файл можно редактировать.

Справа от надписи Станции выводится имя загруженного файла частотных присвоений и находится позиция, которая помечается галочкой, если данные этого файла необходимо использовать (см. раздел 3.6 Редактор частотных присвоении). Двойной щелчок мыши в этой области вызывает закладку Станции панели Настройки, где этот файл можно редактировать.

Справа от надписи Спектры выводится имя загруженного файла библиотеки эталонных спектров.

Двойной щелчок мыши в этой области вызывает закладку

Спектры панели Настройки, где находится редактор библиотек спектров, используемых в качестве эталонов.

Число справа от надписи Фильтры отмечает количество подключенных фильтров-классификаторов сигналов. Двойной щелчок мыши по этой надписи вызывает закладку Фильтры панели Настройки, где их можно настраивать и подключать. В правой колонке отображается число усреднений и состояние аттенюатора приемника. Двойной щелчок мыши в этой области вызывает закладку Панорама панели Настройки, где можно изменять значения этих параметров. Справа от надписи Антенна/Канал выведен номер антенного входа радиоприемника (1 или 2) и номер активного входа антенного коммутатора (1,2,3 или 4). двойной щелчок мыши по этой надписи или нажатие клавиш <CTRL + C> вызывает последовательное переключение каналов коммутатора. Если командой меню выбран один
из режимов Экспресс-анализ или Регистрация, то его название отображается в нижней части этой колонки.

7. Строка названия.

В строке названия (рис. 3.1, позиция 6) выводится название и версия программы, а также имя файла базы данных обнаруженных сигналов, с которым в настоящий момент работает программа. В начале и конце строки расположены кнопки управления основным окном. Щелчок мыши по левой кнопке с пиктограммой программы открывает стандартное окно Windows с командами: Переместить, Размер, Свернуть, Развернуть, Закрыть, которые дублируются стандартными кнопками в правой части строки. Этими кнопками можно развернуть основное окно программы на весь экран или свернуть его для доступа к окнам других программ.

8. Строка меню.

Строка меню (рис. 3.1, позиция 6) содержит разделы Файл, Настройки, База
данных, Режим, Справка.

Рис. 3.3. Строка состояния программы RT2060 с лампой индикации режима, кнопкой Старт/Стоп, индикатором выполнения и областями отображения координат измерительных курсоров

В разделе Файл содержатся команды загрузки и сохранения файлов Открыть (эквивалентная клавиатурная комбинация — <CTRL + O>), Сохранить (клавиши <Ctrl + S>) и Сохранить как, а также команда завершения работы программы Выход (клавиши <A1t + F4>). В панели меню Файл выводятся имена последних четырех файлов, которые открывались программой. Для быстрой загрузки такого файла достаточно щелкнуть мышью по его имени или нажать соответствующий номер на клавиатуре.

Командой Настройки (или функциональной клавишей <F3>) вызывается панель с закладками Фильтры, Вид, Устройства, Панорама, Пороги, Станции, Регистрация и Спектры для ввода параметров управления программой. В разделе База данных содержатся команды удаления записей из базы данных Очистить (клавиши <CTRL +Del>) и Удалить выделенные (клавиша < Del >), а также команда сохранения спектра обнаруженного сигнала в качестве эталона Сохранить спектр (клавиша <Ins>).

Меню Режим содержит команды Экспресс-Анализ (F5), Регистрация (F7) и Генератор, которые служат соответственно для вызова средств ручного и автоматического анализа сигналов, регистрации фонограмм с выхода демодулятора приемника и включения программируемого генератора.

Меню Справка содержит команды вызова справочной системы (клавиша F1) и окна с информацией о разработчике программы.

9. Строка отображения состояния программы.

В левой части этой строки (рис. 3.3), расположенной в нижней части основного окна программы, находится лампочка индикации режима программы (позиция 1), которая горит зеленым цветом в режиме сбора данных радионаблюдения и красным - в режиме обработки. Правее размещена кнопка Старт запуска и выключения режима сбора данных (позиция 2). После включения режима сбора данных накнопке появляется надпись Стоп.

Следующие три области (позиции 3, 4 и 5) выделены для отображения параметров обзора. Счетчик циклов обзора (позиция 3) определяет суммарное число циклов обзора за все время работы программы с определенной базой данных. Текущая загрузка диапазона (позиция 4) равна отношению суммы занятых

сигналами частотных полос ко всей полосе обзора в процентах. Средняя скорость обзора в позиции 5 выражается в МГц/с. Далее расположен индикатор процесса обзора (позиция 6), который отражает степень завершения текущего цикла обзора. Для измерений уровней и частот на экране спектральных панорам и экране спектров обнаруженных сигналов используется курсор мыши. Курсор мыши имеет форму стрелки, если он наводится на любую часть окна программы, кроме экранов, где
он принимает форму перекрестия. При этом в позициях 7,8 и 10, 11 строки сообщений выводятся значения координат курсора, соответствующие частоте и уровню сигналов на экранах соответственно спектральных панорам и спектров. После вывода курсора из пределов экрана его последние координаты сохраняются в области отображения. В позиции 9 выводится текущий номер цикла сканирования в группе циклов, после завершения которого автоматически выполняется обработка данных. При включении программируемого генератора в позиции 12 появляется соответствующая пиктограмма.

Контрольные вопросы

1. Что изображено на экране спектральных панорам?
2. О чем информирует экран спектрограммы?
3. Какая информация выводится на экран отображения спектра?
4. Что представляет собой список обнаруженных сигналов?
5. Что отображает окно индикации параметров управления?
6. Какая информация выводится в строке названия?
7. Что отображает строка состояния программы?

Лабораторная работа № 26-27
Скрытая передача информации в JPEG изображениях

Цель работы: ознакомиться с визуальными искажениями в результате внедрения информации в различные компоненты JPEG изображения.

В ходе работы в изображение 800x600 пикселей внедряется примерно 700 Кбайт информации (роман Льва Толстого “Война и мир” в сжатом виде). Задача выполняющего лабораторную работу - обеспечить, чтобы визуальные искажения изображения при этом были как можно менее заметны.

Методические указания.

В ходе выполнения работы можно указывать программе, в какие компоненты JPEG изображения внедрить больше информации, а в какие меньше. Суммарное количество информации при этом остается прежним и меняется только ее распределение между компонентами изображения.

После любых изменений в настройках нажимайте на надпись «Изображение с внедренным сообщением» и тогда на экран будет выведено это изображение, а справа от него будет выводиться количественная оценка его качества в дБ. Для выполнения лабораторной работы необходимо, чтобы качество было больше 43 дБ. Та подгруппа, у которой значение PSNR (пиковое соотношение сигнал/шум) будет максимальным, получает за выполнение работы 25 баллов. Остальные подгруппы - по 20 баллов.

С помощью ползунка можно выбирать баланс распределения информации между цветовой и яркостной компонентой. Определите, в какой из компонент искажения заметнее?

С помощью ползунка «Маскирование в текстурных участках» можно перераспределять информацию между однородными (небо) участками изображения и текстурными (листья, рябь на воде).

В восьми строках ввода можно для каждого коэффициента ДКП (при JPEG сжатии выполняется дискретное косинусное преобразование в блоках 8x8 пикселей и для каждого блока осуществляется квантование) отдельно задать долю внедрения туда информации. Эти коэффициенты должны быть положительными числами, большими, чем ноль. 0-й коэффициент соответствует самой низкой частоте, а 9-й - самой высокой. Чем больший коэффициент будет задан, тем больше информации будет внедрено в соответствующие частоты изображения. Определите, в каких частотах человеческий глаз лучше замечает искажения?

Лабораторная работа № 28-30

Запись и чтение информации для пластиковых карт с магнитной полосой

Цель работы: ознакомиться с устройством чтения/записи пластиковых карт MSR605. Ознакомиться с принципом программирования работы подобных устройств. Написать программы на языке Matlab для записи информации на кредитную карту и для чтения информации с кредитной карты.

Методические указания.

1. Устройство пластиковой карты с магнитной полосой.

Магнитная полоса - носитель информации с ограниченным объемом памяти. Магнитная полоса может быть изготовлена для различных напряженностей магнитного поля. Поэтому параметру существует различие: LoCo (Low Coercitive - низкокоэрцетивные = 300 эрстед) и HiCo (High Coercitive - высококоэрцитивные = 2750 эрстед) магнитные полосы. Различие между магнитными полосами LoCo и HiCo заключается в силе тока, используемого при намагничивании. Для того, чтобы записать информацию на магнитную полосу LoCo используется ток, силой 300 эрстед. Для полосы HiCo применяется ток, силой 2750 эрстед.

Пластиковые карты с магнитной полосой HiCo более надежны и долговечны, так как информация на магнитных полосах HiCo менее подвержена размагничивается внешними магнитными полями, чем на полосах LoCo. Магнитная полоса HiCo используется в тех случаях, когда требуется защитить информацию на магнитной карте от возможного размагничивания, а также повысить защищенность карт от возможной подделки. Карты с магнитной полосой HiCo стоят дороже, чем карты с магнитной полосой LoCo. Например, для дисконтной системы (когда карта используется относительно редко) выбирается магнитная полоса LoCo.

Для промышленного предприятия, где магнитная карта используется работниками ежедневно для прохода через проходную, выбирается магнитная полоса HiCo.

По цвету магнитные полосы различаются следующим образом: HiCo - полоса черного цвета, LoCo - полоса коричневого цвета.

Магнитная полоса предполагает машинное считывание. Для стандартных считывающих устройств (ридеров) магнитная полоса делается шириной 12,7 мм (0,5 дюйма) и располагается на расстоянии 4 мм о т края карточки.На магнитной полосе находится три дорожки, по которым можно нанести ту или иную информацию. Все три дорожки магнитной полосы используются, как правило, в крупных банковских платежных системах (например, VISA).

В дисконтных системах, в локальных платежных системах, а также в системах доступа используется чаще всего одна дорожка (обычно вторая).

1- дорожка - цифробуквенная информация: до 76 знакомест QWERTYUIOPASDFGHJKLZXCVBNM1234567890 : ; = + ( ) “ ‘ ! @ # л & * < > /. Все латинские буквы заглавные .Информация будет окружена служебными символами:" % " в начале строки, " ? " в конце строкиСлужебный знак „?” добавляется в конце каждой строки базы данных и означает конец записи на магнитную полосу и при считывании не отображается.

2- дорожка - только цифры: 1234567890 и знак до 37 знакомест пробел отображается на магнитной полосе знаком „=”, знак „?” означает конец записи на магнитную полосу и при считывании не отображается. Информация будет окружена служебными символами:" ; " в начале строки, " ? " в конце строки

3- дорожка - только цифры: 1234567890 и знак „=”, до 104 знакомест пробел отображается на магнитной ленте знаком „=”, знак „?” означает конец записи на магнитную ленту и при считывании не отображается. Информация будет окружена служебными символами:" _ "в начале строки, " ? " в конце строки

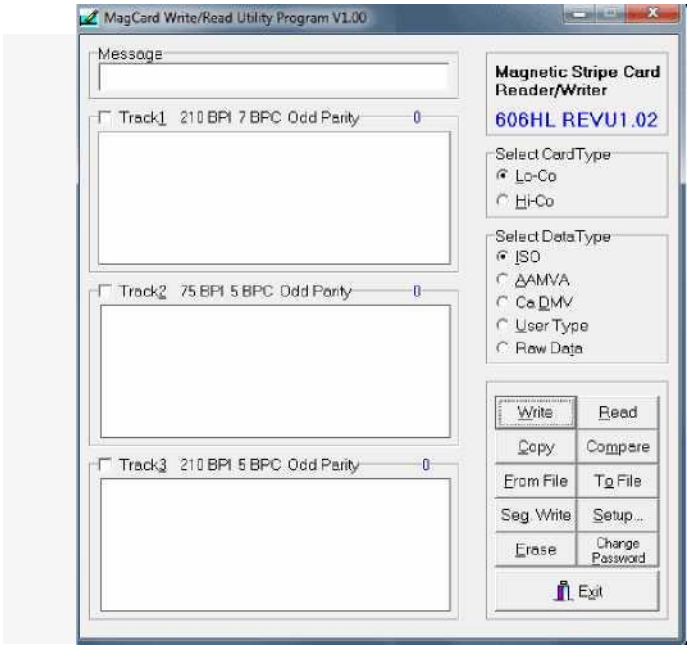
2. Описание MSR605.

Энкодер MSR606 поддерживает чтение и запись трех треков карт высокой (HI-CO) и низкой (LO-CO) намагниченности стандартов ISO 7811-7816, AAMVA и других. Энкодер питается от 24v постоянного тока и в наборе предусмотрен универсальный блок питания, работающий от сети 110-240v переменного тока. Подключается энкодер посредством USB кабеля.

Работа с софтом

При первом запуске программа попросит ввести пароль для дальнейшего использования. Его можно не вводить, но при каждом запуске это окно будет все равно появляться, а убрать его нельзя.

После ввода пароля (или закрытия окна) программа проинициализирует энкодер, после чего с ним можно будет начинать работать. О состоянии готовности энкодера можно судить по горящему зеленому светодиоду на панели энкодера и наличию названия модели и ревизии



Слева три больших текстовых поля, именуемых Track 1, 2 и 3 служат для отображения содержимого соответствующего трека считываемой карты. Также туда можно ввести свои данные для записи на соответствующий трек карты. Заголовок каждого поля, помимо номера трека, указывает плотность данных в битах на дюйм, кодировку символов (с учетом бита четности), тип четности и размер данных.

В разделе "Select Card" Type можно выбрать намагниченность (coercivity) карты, с которыми предстоит работать. Данную опцию стоит выбирать при операциях с записью или стиранием карты, при чтении карты любой намагниченности читаются одинаково независимо от выбранной опции. При переключении типа намагниченности в самом энкодере раздается характерный щелчок.

В разделе "Data Type" можно выбрать тип используемых данных. Данная возможность больше представлена для удобства пользователя, автоматически переводя нули и единицы в удобный для просмотра и редактирования формат. Формат ISO применяется в основном при работе с кредитными и банковскими картами, а форматы AAMVA и Ca DMV соответствуют типу данных, используемых соответственно американской ассоциацией транспортных средств и департаментом транспортных средств шт. Калифорния. Форматы могут отличаться плотностью данных на каждом треке, кодировкой и наличием или отсутствием четности. Тип "User Type" позволяет настроить формат под себя, если он не совместим с первыми тремя форматами, а тип "Raw Type" используется в том случае, когда параметры формата неизвестны или используется нестандартный формат. В таком случае данные с треков переводятся в шестнадцатеричный формат из нулей и единиц.

В нижнем разделе представлены кнопки для работы с энкодером. Основные из них - Read, Write, Erase говорят сами за себя и отвечают, соответственно, за чтение, запись и стирание карт.

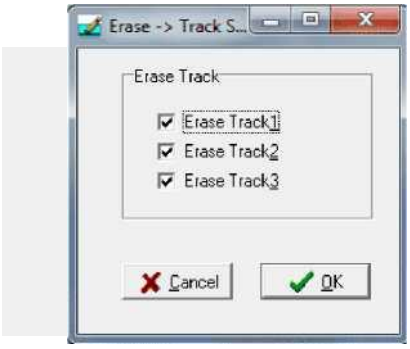
При выборе функции чтения энкодер переходит в режим "Ready" (загорается желтый

операцию, программа будет указывать сколько карт было обработано за текущую сессию.

При записи программа ведет себя аналогично, только на энкодере в режиме ожидания горят одновременно зеленый индикатор "Ok" и желтый "Ready". В энкодере читающая головка находится после записывающей, поэтому записанные данные сразу же проверяются. В случае успешной записи загорается только зеленый светодиод и энкодер сразу переходит снова в режим ожидания. Если же во время записи или другой операции произошла ошибка, то на энкодере загорится красный светодиод, а программа оповестит об ошибке.

Ошибка может произойти в случае использования поврежденной карты, при попытке записать карту высокой намагниченности, когда выбрана опция "Lo-Co", при неравномерном проведении карты через энкодер или когда загрязнятся головки энкодера.

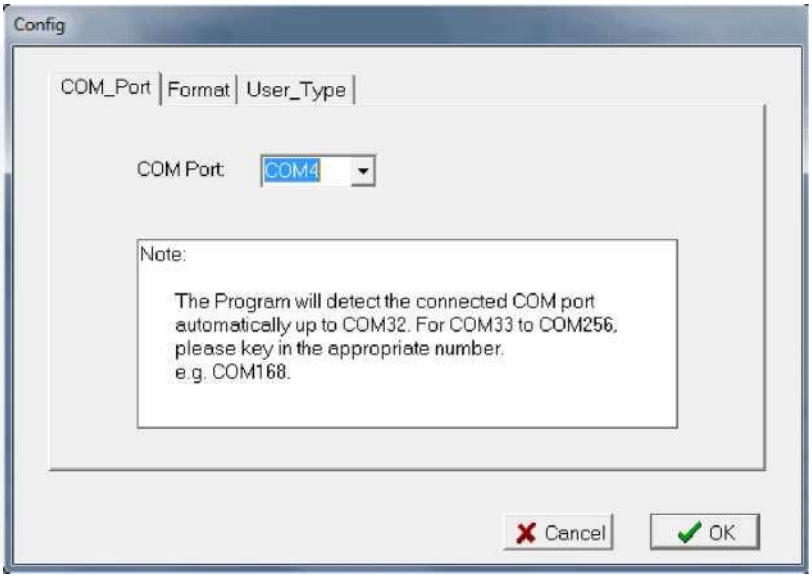
Функция "Erase" позволяет стереть выбранные треки на карте. Стирать карту лучше всегда перед записью новых данных, несмотря на то, что в большинстве случаев перезапись данных проходит успешно без предварительного стирания.



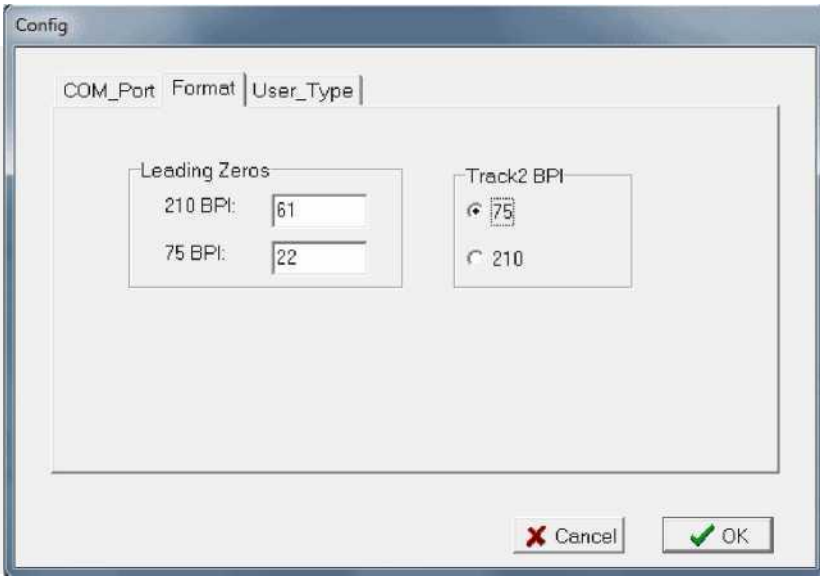
"Copy" дает нам возможность считать одну карту и изготовить дубликаты. Compare используется для сравнения идентичных карт и в случае несоответствия прочитанных данных программа оповестит об ошибке.

"To File" используется для пакетной записи данных в файл. При этом в файл записывается дата и время и данные выбранных треков. Для пакетной записи сохраненных данных используется уже "From File".

"Setup" дает настроить основные параметры работы программы. На вкладке "Com Port" можно выбрать используемый порт для связи с энкодером. Как видите, выбор довольно широк



На вкладке Format type можно вручную настроить количество ведущих нулей и



И на последней вкладке можно настроить те самые параметры данных, которые будут учитываться при чтении или записи нестандартных типов карт, если была выбрана опция "User Type" в разделе "Data Type".

3. Принципы программирования MSR605. Перечень и описание функций на языке Matlab (подготовленных для облегчения выполнения лабораторной работы).

Для выполнения лабораторной работы необходимо открыть папку MSR с подготовленными файлами, для облегчения работы, которые разработаны в среде Matlab. В папке находятся файлы: msr_start.m, msr_open.m, zapis.m, chtenie.m, msr_close.m.

Файл msr_open.m подключает COM-порт(если номер порта не совпадает, нужно зайти в диспетчер устройств, пункт Ports(COM&LPT) покажет к какому порту подключен энкодер, и в файле msr_open.m изменить значение на свой порт).

Файл zapis.m производит запись на три дорожки магнитной карты. После запуска msr_start.m и msr_open.m необходимо ввести строку:

“zapis(msrf,msr,'ABCDEF 1234567890798765434532','1234234534');”

После ввода строки загориться зеленая и желтая лапочки которые оповещают что нужно провести карту. После проведения карточки энкодер запишет на три дорожки все те элементы которые находятся в кавычках (каждые кавычки соответствуют одной дорожке).

Файл chtenie.m отвечает за чтение данных с магнитной карты. Для чтения необходимо прописать строку “chtenie(msrf,msr);”, после чего на энкодере должна загорется желтая лампочка, которая информирует о том что нужно провести карту. После того как будет проведена карта, в поле Matlab должны появиться данные которые мы записывали на карту.

Файл msr_close.m подключается для завершения работы с энкодером, он отключает COM-порт.

Примечание: заводская программа msr605 и Matlab не могут работать вместе, их стоит включать поочередно. При работе с Matlab необходимо обязательно заканчивать работу файлом msr_close.m, так как порт будет занят и заводская программа не сможет работать с энкодером.

4. Ход выполнения лабораторной работы.

1) Ознакомьтесь с устройством MSR605, прилагаемым ПО. Попробуйте прочитать и записать информацию с помощью этого ПО.

2) Ознакомьтесь с руководством программиста (файл “MSR605 Programmer's Manual.pdf”).

3) Ознакомьтесь с прилагаемым набором подпрограмм для Matlab по облегчению работы с MSR605.

4) Напишите программу на Matlab, которая включит красную лампочку на устройстве. Подождите, пока пользователь нажмет клавишу (команда “pause” Matlab) и выключите красную лампочку, а включите зеленую. Найдите в руководстве программиста соответствующие последовательности, которые нужно послать на MSR605.

5) Модифицируйте прилагаемые программы “zapis.m” и “chtenie.m” так, чтобы записывалась и читалась только третья дорожка карты.

6) На третью дорожку можно записывать только цифры от 0 до 9 (не больше 104 цифр). Напишите программу, которая бы позволила писать на эту дорожку русские буквы. Для этого используйте следующую идею. Каждую русскую букву можно представить в виде пары цифр. Например букву “А” можно представить как “00”, букву “Б” как “01”, букву “В” как “02” и так далее. Буква “И” будет кодироваться как “10”, “К” - как “11”, “Л” - как “12”. Всего в русском алфавите 33 буквы. Поэтому большие русские буквы будут кодироваться парами цифр от “00” до “32”, маленькие буквы парами цифр от “33” до “55”. Еще один код “56” можно отвести на кодирование пробела. Напишите функцию для перекодирования текстовой строки из букв в пары цифр и функцию для перекодирования строки из пар цифр в буквы. Закодируйте с помощью написанной Вами функции свои имя, фамилию и отчество (на русском языке) и запишите их на третью дорожку карты.

Лабораторная работа 32-35
Виды штрих-кодов, их генерация и считывание

Цель работы

Ознакомиться с программированием контактных смарт-карт и построением СКУД на базе контактных смарт-карт.

Учебный материал
5. Штрих-коды
Штрих-код – графическая информация, наносимая на поверхность изделий, представляющая возможность считывания еѐ техническими средствами — последовательность чѐрных и белых полос либо других геометрических фигур. Линейными (обычными) называются штрихкоды, читаемые в одном направлении (по горизонтали). Наиболее распространѐнные линейные символики: EAN (EAN-8 состоит из 8 цифр, EAN-13 — используются 13 цифр), UPC (UPC-A,UPC-E), Code56, Code128 (UPC/EAN-128). Линейные символики позволяют кодировать небольшой объѐм информации (до 20—30 символов, обычно цифр).
Двухмерные символики были разработаны для кодирования большого объѐма информации. Расшифровка такого кода проводится в двух измерениях (по горизонтали и по вертикали). Многоуровневые штрихкоды появились исторически ранее, и представляют собой поставленные друг на друга несколько обычных линейных кодов. Матричные же коды более плотно упаковывают информационные элементы по вертикали.
5.1. Линейные штрих-коды
1. UPC или Universal Product Code (универсальный код товара) — американский стандарт штрих-кода, предназначенный для отслеживания товаров в магазинах.
Разновидности кода:
UPC-A (полный) — кодируется 12 цифр.
UPC-E (сокращѐнный) — кодируется 8 цифр.
Код UPC содержит только числа и никаких букв или других символов.
Код UPC — простой и практически симметричный линейный штрих-код. Эта простота, симметричность и высокая помехозащищѐнность обусловлена недостаточно развитой техникой времѐн создания этих кодов. Код состоит из 2 групп цифр, по 6 цифр в каждой группе — левой и правой. Группы цифр окаймляются так называемыми защитными, или ограждающими, штрих-шаблонами (Guard Patterns). Эти шаблоны содержат штрихи единичной ширины, которые служат для синхронизации сканера штрих-кода. Наличие именно трѐх таких полей обусловлено в первую очередь возможным нанесением штрих-кода на закруглѐнную поверхность. И если сейчас это не является особой проблемой, то во времена создания этого кода сканеру требовалось знать ширину единичного штриха в начале, середине и конце кода. Левые и правые защитные шаблоны состоят из 3 штрихов единичной ширины — двух тѐмных и одного светлого между ними. Средний защитный шаблон
состоит из 5 штрихов — трѐх светлых и двух тѐмных. Всѐ остальное — цифры.
Каждая цифра левой или правой группы кодируется с помощью четырѐх штрихов: двух светлых и двух тѐмных. Каждый штрих может иметь относительную ширину в одну, две, три или четыре единицы. Общая ширина штрихов для одной цифры всегда составляет семь единиц. Битовая комбинация для каждой цифры разработана таким образом, чтобы цифры, насколько это возможно, отличались друг от друга. Максимальная длина тѐмного или светлого участка не может превышать четырѐх единиц. Общая ширина всего кода всегда равна 95 единицам. В любом коде 29 светлых и 30 тѐмных штрихов. Все эти технические решения очень важны для надѐжности и простоты сканирования этого кода.
Первая цифра кода — это так называемый префикс — имеет некоторое логическое значение, но не столь важна с технической точки зрения. Последняя цифра — контрольное число,

служит для выявления возможной ошибки при чтении кода сканером или ручного ввода цифр кода с клавиатуры.
Направление чтения комбинации штрихов значения не имеет, код специально разрабатывался так, чтобы он одинаково просто считывался как в прямом, так и обратном направлении (если товар перевѐрнут). Также не имеет значения то, какое исполнение имеет весь штрих-код — фотографически позитивное или негативное. То есть штрих-код, нанесѐнный светлыми полосками по тѐмному фону читается абсолютно так же, как и тѐмными полосками по светлому фону. Мало того, цвета штрихов и фона не обязательно должны быть белыми и чѐрными, возможны и другие цветовые комбинации.

5.2. Кодировка цифр

При проектировании структуры кода, в условиях ещѐ не слишком развитой электроники, было важным сделать его как можно более простым для считывания сканером и упростить аппаратную часть самого сканера. Одной из сложностей была проблема вероятного считывания кода в обратном направлении, то есть считывания кода на товаре, который кассир поднѐс к сканеру «вверх ногами». Поэтому очень важно было, чтобы чередование полос было одинаковым в обоих направлениях — сначала тѐмный штрих, потом белый, потом опять тѐмный и так далее. Да, и ещѐ было бы неплохо, чтобы положение защитных шаблонов было всегда на одном и том же месте.
Решение было найдено. Можно обратить внимание, что код выглядит очень симметрично, то есть количество штрихов справа и слева от центра всегда
равно, а ширина правой и левой части штрих-кода одинаковы. То есть механизм считывания штрих-кода всегда одинаков, как этот код ни поверни.
Что касается одинаковой последовательности чередования светлых и тѐмных штрихов при прямом и обратном чтении, то разработчики добились этого тем, что кодировка правой и левой групп цифр немного отличается — правые символы имеют фотографически негативное начертание относительно левых. То есть шаблоны штрихов для одной и той же цифры идентичны, но позитивны или негативны. Иначе говоря, отличие только в том, что если для левой части кода это светлый штрих, то для правой — тѐмный.
Проблема распознавания прямого или обратного считывания точно так же легко разрешается логически. Например, если сканер считывает цифру с толщиной штрихов 3-2-1-1, то он понимает, что это цифра «ноль» и еѐ прямое считывание, а если он считывает штрихи толщиной 1-1-2-3, то он понимает, что это тот же «ноль», но считанный в обратном направлении. Считывая числа, закодированные зеркально относительно обычной кодировки, сканер понимает, что весь штрих-код считывается в обратном направлении, следовательно, и всю полученную последовательность из 12 цифр нужно передать компьютеру в обратном порядке.
В коде UPC-A (GTIN-12) контрольное число (цифра) рассчитывается следующим образом:
Суммируются все цифры на нечѐтных позициях (первая, третья, пятая, и т. д.) и результат умножается на три.
Суммируются все цифры на чѐтных позициях (вторая, четвѐртая, шестая, и т. д.).
Числа, полученные на предыдущих двух шагах, складываются, и из полученного результата оставляется только последняя цифра.
Эту цифру вычитают из 10.
Конечный результат этих вычислений и есть контрольная цифра (десятке соответствует цифра 0).
Например, контрольное число для приведѐнного на рисунке штрих-кода UPC-A «03600029145X», где «X» — это искомая контрольная цифра, рассчитывается путѐм сложения всех нечѐтных цифр (0+6+0+2+1+5 = 14), умножается на три (14 × 3 = 42), результат суммируется со всеми чѐтными цифрами (42+3+0+0+9+4 = 58), отбрасывается всѐ, кроме последней цифры (58 mod 10 = 8), вычитается из 10 (10 − 8 = 2) и ещѐ раз, если это необходимо, отбрасывается всѐ, кроме последней цифры (2 mod 10 = 2). Искомое контрольное число — цифра 2.

При считывании кода правильность считывания проверяется похожим способом, но несколько проще:
суммируются все чѐтные цифры, включая контрольную цифру.
суммируются все нечѐтные цифры и умножаются на 3.
эти суммы складываются и оставляется последняя цифра от результата.
Технически цифры обрабатываются последовательно, за один проход, с умножением каждой цифры на 1 или 3, в зависимости от чѐтности позиции, добавлением к сумме и взятием остатка по модулю 10 от текущей суммы. Иными словами десятки сразу отбрасываются, что сильно упрощает механизм вычисления.
Если результат равен нулю, то принимается решение, что код считан правильно, если любая другая цифра, то код однозначно считан неверно.

5.3. Кодировка товара

Данный код создавался, в первую очередь, для автоматизации торговли продукцией, произведѐнной множеством предприятий, поэтому вопрос внутреннего содержания также был важен для стандартизации и регулирования, чтобы разные предприятия не могли присвоить товару одинаковый код. Каждый вновь производимый вид товара должен был иметь свой уникальный код, и это было главной задумкой всей этой системы. То есть, если производитель выпускает, например, джинсы, то джинсы разного цвета, размера, покроя, должны были иметь различные коды. То есть, если это, например, 10 цветов, 50 видов, 20 размеров, то для их кодировки потребуется десять тысяч кодов.
В свою очередь одинаковый товар, но разных предприятий-производителей, тоже должен был иметь различную кодировку. Всѐ это было важно для автоматизации учѐта в торговле, автоматического контроля остатков товара на складе, прилавках магазинов и так далее.
Теоретический максимум этого кода — 100 миллиардов различных видов товара (11 цифр). Казалось бы, огромное число. Но теория не всегда соответствует практике, и нынешняя ситуация такова, что, более чем за 30 лет существования системы, этих кодов оказалось недостаточно. Это связано с несбалансированным, расточительным их расходованием.
Первоначально 11 цифр кода были распределены следующим образом:
Префикс — 1 цифра.
Код производителя — 5 цифр.
Код товара — 5 цифр.
То есть, теоретически система подразумевала до шестисот тысяч предприятий (по сто тысяч на префикс), каждое из которых могло кодировать до ста тысяч наименований выпускаемой им продукции.

Префикс
Это первая цифра кода. Логически делит коды на виды выпускаемой продукции.
0, 1, 6, 7, 8 — для большей части товаров.
2 — Зарезервировано для внутреннего использования торговыми предприятиями, для весовых товаров. Переменная весовая часть кода UPC для таких товаров, как сыры, колбасы, свежие фрукты и других присваивается в магазине во время их упаковки. При этом левая часть кода — это внутренний код товара в этом магазине, а в правой части кода указывается вес или цена. Магазин сам определяет, как кодировать такой товар.
3 — Медикаменты и прочая продукция фармацевтики, согласно американскому коду National Drug Code (NDC).
4 — Зарезервировано для внутреннего использования торговыми предприятиями для карт покупателя.
5 или 9 — для купонов, но многие торговые предприятия игнорируют это.
Для европейских кодов EAN-13 все эти американские префиксы представляются начинающимися с нуля, то есть 01, 02, 03 и так далее. После объединения с европейской ассоциацией в глобальную GS1 Америке были присвоены дополнительные префиксы 10-13 в европейской кодировке, которые будут использоваться для кодировки обычного товара.

Код предприятия

Код предприятия — это та часть кода, которая присваивается регулирующей организацией предприятиям, желающим кодировать свой товар. Код предприятия, по-первоначальному замыслу, должен был занимать 5 цифр плюс префиксы, отведѐнные под кодирование обычного товара. Таким образом, можно было зарегистрировать порядка шестисот тысяч предприятий. Как оказалось, этого мало. Код предприятия располагается в левой части кода UPC.

Код товара

Код товара занимает 5 первых цифр правой части кода. Каждый вид товара предприятие должно было кодировать своим, уникальным кодом. Код 99999
зарезервирован для кодировки самого предприятия, в целях обеспечения автоматизации документооборота.

Кодировка товара

Смысловая нагрузка цифр в наименовании товара: Вопреки сложившемуся мнению, цифровой код самого товара (3-5 цифр) никакой смысловой нагрузки не несѐт. Ассоциация рекомендует последовательное присвоение кодов по мере выпуска новых видов продукции без вложения в этот код какой либо дополнительной смысловой нагрузки.

Для использования UPC внутри предприятий и торговых организаций выделяются все коды, начинающиеся с цифры 2. Любое предприятие может использовать их как угодно и по своему усмотрению, но исключительно в своих внутренних целях. Использование этих кодов за пределами предприятия запрещено. Внутреннее содержание кодов, начинающихся с 2, может подчиняться любой логике, которое установило то или иное предприятие для себя (обычно это предприятия розничной торговли), и может содержать цену или вес товара, или любые другие параметры, и особенно часто эта кодировка применяется для весового товара.

2. European Article Number, EAN (европейский номер товара) — европейский стандарт штрихкода, предназначенный для кодирования идентификатора товара и производителя. Является надмножеством американского стандарта UPC.

Разновидности кода:

EAN-8 (сокращѐнный) — кодируется 8 цифр.

EAN-13 (полный) — кодируется 13 цифр.

EAN-128 — кодируется любое количество букв и цифр, объединенных в регламентированные группы.

Коды EAN-8 и EAN-13 содержат только цифры и никаких букв или других символов. Например: 2400000032639. Кодом EAN-128 кодируется любое количество букв и цифр по алфавиту Code-128. Например:(00)353912345678(01)053987(15)051230, где (15) группа обозначает срок годности 30 декабря 2005.

Первоначально была разработана американская система штрихового кодирования Universal Product Code. Статью об этом коде настоятельно рекомендуется изучить перед чтением последующего текста. В текущей же статье пропущена та часть информации, которая для обоих кодов является идентичной, и данная статья больше описывает отличия и особенности EAN-13 по сравнению с UPC.

Разработанная и внедрѐнная система кодировки товаров UPC в США и Канаде стала настолько популярной в супермаркетах, что европейцы также задумались о ее внедрении. Стояло две задачи: обеспечить производителей определѐнным диапазоном кодов, отличных от американских, для кодировки производимых товаров и обеспечить возможность магазинам считывать как американские, так и европейские коды, причем желательно, чтобы на упаковке был только один, единый штрихкод, а не два кода (для США и для Европы). Для того, чтобы закодировать в коде товары других стран, необходимо было увеличить количество разрядов кода с 12 цифр, которые были в эксклюзивном

владении американцев и канадцев до, как минимум, 13 цифр, чтобы использовать эту дополнительную, и первую по счѐту цифру в коде в качестве условного сигнала для торговых программ, что этот товар не американского производства.
Американцам и канадцам в качестве этой цифры разработчики сразу зарезервировали ноль. У европейцев стояла и организационная задача: распределить (делегировать) определѐнные диапазоны значений кодов различным странам мира, для чего определили в качестве префикса региона первые три цифры, включая дополнительную тринадцатую. Вопреки заблуждению, этот префикс не означает страну происхождения товара, а лишь указывает код регионального регистратора, где зарегистрировалась компания, печатающая код на своей упаковке. Товар может быть произведѐн, например, в Китае, но китайская компания, зная, что товар в этой русскоязычной упаковке будет продаваться в России, законно может зарегистрировать для себя коды в российской организации GS1, и выпускать продукцию со штрихкодом, начинающимся с 460—469. И наоборот, товар может быть выпущен в России, а код может быть использован не российский. Однако чаще всего в качестве регионального кода действительно встречается код той страны, где выпущен данный товар.
Помимо организационной задачи, перед разработчиками стояла серьѐзная техническая задача — сохранить совместимость кодов и одновременно возможность минимальных аппаратно-программных переделок сканеров штрихкода, тогда ещѐ достаточно дорогих. Важно было сохранить то же самое количество штрихов, осевую симметричность кода для его удобного чтения как в прямом, так и в обратном направлении (если товар поднесѐн к сканеру «вверх-тормашками»), возможность чтения негативных кодов (светлые штрихи на тѐмном фоне). В результате было найдено простое решение: в целях максимальной совместимости кодирование EAN было переработано из UPC так, что по-прежнему содержало только 12 «штриховых цифр» (то есть только 12 цифр в коде имеют соответствие конкретным штрихам), а дополнительная тринадцатая цифра вычислялась логическим путѐм. «Рисунок» EAN-13 ничем не отличается от рисунка UPC, а для кодов, начинающихся с нуля был точной копией.

Структура кода EAN-13

Первая цифра	Первая (левая) группа из 6 цифр	Вторая (правая) группа из 6 цифр
0	LLLLLL	RRRRRR
1	LLGLGG	RRRRRR
2	LLGGLG	RRRRRR
3	LLGGGL	RRRRRR
4	LGLLGG	RRRRRR
5	LGGLLG	RRRRRR
6	LGGGLL	RRRRRR
7	LGLGLG	RRRRRR
8	LGLGGL	RRRRRR
9	LGGLGL	RRRRRR

Первая цифра кодируется не дополнительными штрихами, а способом кодирования левой половины штрих-кода (10 разновидностей). Из таблицы видно, что для кодирования первой цифры используется немного разное начертание штрихов, обозначенное буквами L и буквами G. Определѐнное чередование этих кодов даѐт сканеру на уровне логики определить 13 цифру. Например, для цифры «1» G-код у третьей, пятой и шестой цифры, то есть встретив код, в котором G-код левой части кода расположен в этом порядке, сканер в качестве первой цифры передаст в компьютер единицу. Для цифры

«2» G-код у третьей, четвѐртой и шестой цифры, соответственно сканер передаст в компьютер двойку. Для других цифр эта логика отображена в таблице.

Кодирование цифр

Цифра	L-код	R-код	G-код
0	0001101	1110010	0100111
1	0011001	1100110	0110011
2	0010011	1101100	0011011
3	0111101	1000010	0100001
4	0100011	1011100	0011101
5	0110001	1001110	0111001
6	0101111	1010000	0000101
7	0111011	1000100	0010001
8	0110111	1001000	0001001
9	0001011	1110100	0010111

Графические отличия L-кода, R-кода и G-кода состоят в следующем. Для каждой цифры это одна и та же комбинация чѐрно-белых штрихов, L-код отличается от R-кода лишь фотографически негативным исполнением, а G-код отличается от R-кода реверсивным (зеркальным) исполнением.

Для цифры 0 в коде ни для одной из шести цифр левой части кода нет ни одного преобразования в зеркально-негативный вид, то есть все штрихи кодируются L-кодом, как в UPC. EAN-сканер, встретив код без штрихов с G-кодом, передаѐт в компьютер первую цифру 0. В свою очередь, если этот код прочитает уже редко применяемый сканер штрихкодов UPC, то он будет просто прочитан как «родной» код UPC. Если же сканер UPC встретит на своѐм пути штриховку с G-кодом, то он не сможет считать этот код и выдаст ошибку или не заметит и не передаст в компьютер никакого кода. Этим и обеспечена полная совместимость «снизу-вверх».

Таким образом, UPC может считаться частным случаем, подмножеством кода EAN-13, у которого первая цифра есть 0 и которая часто не указывается в виде арабской цифры, тогда эти коды ничем не отличаются друг от друга по рисунку. Была полностью сохранена возможность чтения «американских» кодов на «европейских» сканерах, но не наоборот. Код EAN-13 и его 13-я цифра в свою очередь формируется «игрой» негативности-реверсивности последовательности штрихов в левой части кода, в результате чего «американские» сканеры UPC читать европейский код не в состоянии, но обеспечена максимальная «похожесть» кодов друг на друга. С течением времени в США и Канаде этот тип сканеров уже вытеснен из магазинов, и установлены сканеры, способные считывать кодировку EAN-13, поэтому продажа товаров из других стран не вызывает проблем на их территории.

EAN-8

Использование штрих-кодов EAN-13 хотя и удобно, но не всегда возможно. Если товар имеет малые размеры, то для кода EAN-13 может не найтись достаточно места на этикетке. Уменьшение размера кода приводит к уменьшению ширины штрихов. Если штрихи будут слишком узкими, разрешающей способности сканера может оказаться недостаточно для уверенного считывания этого штрих-кода. Для маркировки небольших товаров разработан

стандарт штрих-кода EAN-8, в теле сообщения которого кодируется только 8 цифр вместо 13.
Как показывает практика, кодом EAN-8 часто маркируются и достаточно большие по размеру товары. Причина такой маркировки не ясна.
Каждая цифра в EAN-8, как и в EAN-13, кодируется с помощью четырѐх штрихов: двух белых и двух чѐрных. Штрихи могут иметь относительную ширину в одну, две, три и четыре единицы. Общая ширина штрихов одной цифры составляет семь единиц. Направление чтения комбинации штрихов значения не имеет.

EAN-128 (GS1-128)

Данный формат предназначен для передачи информации о грузе между промышленными предприятиями. В коде регламентирован словарь (Code-128) и группы кодов, но не регламентирована длина. Такой код может содержать различную информацию, например, код товара, сроки годности, размеры, объем, код партии производителя и др.
Стандарт штрихкода Code 128 существенно отличается от таких широко распространѐнных стандартов штрихового кода, как например, EAN. Отличия заключаются, прежде всего, в возможности кодирования не
только цифр, но и букв латинского алфавита, а также специальных символов. Кроме того, цифровой код в формате Code 128 становится очень компактным, что достигается за счѐт «двойной упаковки» данных, когда два числа записываются в один модуль штрихкода. Буквенные символы кодируются обычным — «одиночным» способом, что делает буквенный код в формате Code 128 вдвое длиннее цифрового.
Штриховой код Code 128 включает в себя 107 символов. Из которых 103 символа данных, 3 стартовых, и 1 остановочный (стоп) символ. Для кодирования всех 128-ми символов ASCII предусмотрено три комплекта символов штрихового кода Code 128 — A, B и C, которые могут использоваться внутри одного штрихкода.
128A — символы в формате ASCII от 00 до 95 (цифры от «0» до «9» и буквы от «A» до «Z») и специальные символы;
128B — символы в формате ASCII от 32 до 127 (цифры от «0» до «9», буквы от «A» до «Z» и от «a» до «z») и специальные символы;
128C — символы в формате ASCII от 00 до 99 (только для числовых кодов).
Технические требования к символике штрихового кода Code 128, показатели символики, кодирование знаков данных, размеры, алгоритмы декодирования, параметры применения и строки-префиксы и идентификатора символики в России регламентируются ГОСТ 30743-2001 (ИСО/МЭК 15417—2000) «Автоматическая идентификация. Кодирование штриховое. Спецификация символики Code 128 (Код 128)».
Структура штрихкода Code 128 достаточно проста. Штрихкод состоит из шести зон:
Белое поле;
Стартовый символ (Start);
Кодированная информация;
Проверочный символ (контрольный знак);
Остановочный (Stop) символ;
Белое поле.
Символы штрихового кода Code 128 состоят из трѐх штрихов и трѐх промежутков. Штрихи и промежутки имеют модульное построение. Ширина каждого модуля составляет от 1 до 4 модулей (1 модуль = 0,33 мм). Ширина знака равна 11 модулям. Остановочный (стоп) знак состоит из тринадцати модулей и имеет четыре штриха и три промежутка.
В спецификации Code 128 использование контрольного знака является обязательным. Согласно таблице символов штрихкода Code 128, каждому знаку присваивается соответствующие значение. Затем, для каждого знака, кроме знака «Stop» и контрольного знака, назначается весовой
коэффициент, 1, 2, 3,…, n. При этом, знакам «Start» и следующему за ним первому знаку, присваивается весовой коэффициент равный 1. Контрольный знак вычисляется как сумма

произведений весовых коэффициентов на соответствующие значения по модулю 103. Располагается контрольный знак между последним знаком данных и знаком «Stop».

5.4. Двумерные(2D) коды

1. QR-код (англ. quick response — быстрый отклик) — матричный код (двумерный штрихкод), разработанный и представленный японской компанией «Denso-Wave»[1] в 1994 году.

Основное достоинство QR-кода — это лѐгкое распознавание сканирующим оборудованием (в том числе и фотокамерой мобильного телефона), что дает возможность использования в торговле, производстве, логистике.

В отличие от старого штрих-кода, который сканируют тонким лучом, QR-код определяется сенсором как двумерное изображение. Три квадрата в углах изображения позволяют нормализовать размер изображения и его ориентацию, а также угол, под которым сенсор относится к поверхности изображения. Точки переводятся в двоичные числа с проверкой по контрольной сумме.

2. Aztec Code — двумерный матричный штрихкод. Разработан в 1995 году доктором Andrew Longacre, Jr., исследователем из фирмы Welch Allyn Inc. Код был опубликован фирмой AIM International в 1997 году, и хотя на код был получен патент, он был передан в общественное достояние.

Благодаря навигационным маркерам код не зависит от пространственной ориентации, и может быть считан не только при любом угле поворота, но и даже при зеркальном отражении рисунка.

Размер кода может варьироваться от квадрата 15x15 до квадрата 151x151. Наименьший может содержать в себе до 13 цифр или 12 букв английского алфавита, а наибольший — 3832 цифр или 3067 букв английского алфавита или 1914 байт данных. При этом не требуется пустого пространства вокруг рисунка кода.

Наличие особой системы разметки, мишени, также называемой Bullseye, позволяет считывать информацию даже с искажѐнного изображения. Например, повѐрнутого или растянутого.

В коде применяется кодирование Рида-Соломона, позволяющее успешно считывать код при частичном повреждении его поверхности. Стандартный уровень избыточности при кодировании 23 %, при этом его можно изменять от 5 % до 95 %.

Радиальное расположение слоѐв информации позволяет увеличивать объѐм хранящейся информации, просто расширяя область кодирования.

3. PDF417 (англ. Portable Data File — переносимый файл данных) — двумерный штрихкод, поддерживающий кодирование до 2710 знаков. PDF417 был разработан и введен в 1991 году фирмой Symbol Technologies. В настоящее время PDF417 широко применяется в идентификации личности, учѐте товаров, при сдаче отчетности в контролирующие органы и других областях. Формат PDF417 открыт для общего использования.

PDF417 может содержать до 90 строк. Каждая строка состоит из:

стартового и стопового шаблона. Они характеризуют штрихкод как PDF417.

набора ключевых слов (КС):

левый и правый индикаторы — содержат информацию о номере строки, количестве строк и столбцов, уровне коррекции ошибок;

до 30 КС данных, содержащих как непосредственно данные, так и информацию для восстановления поврежденных КС.

Каждое КС состоит из 4 штрихов и 4 пробелов, ширина КС в 17 раз больше минимального штриха или пробела — отсюда числовой суффикс в обозначении формата PDF417.

PDF417 поддерживает три типа данных: текст (ASCII), байты и числа.

PDF417 предусматривает полиноминальное кодирование Рида-Соломона дополнительных данных для восстановления информации. Количество дополнительных КС зависит от уровня коррекции ошибок.

4. DataMatrix — двумерный матричный штрихкод, представляющий собой чѐрно-белые элементы или элементы нескольких различных степеней яркости, обычно в форме квадрата, размещѐнные в прямоугольной или квадратной группе. Матричный штрихкод предназначен для кодирования текста или данных других типов - С помощью DataMatrix можно закодировать как текст, так и другие типы данных — веб-ссылки, адреса электронной почты, телефонные номера и SMS. Код применяется для маркировки в электронике, автомобилестроении, пищевой промышленности, авиакосмической и оборонной промышленности, энергетическом машиностроении. Чаще всего в промышленности и торговле применяются битовые матрицы, кодирующие от нескольких байт до 2 килобайт данных

Ход работы

1) Изучите соответствующий раздел в методическом пособии.
2) Использую утилиту для сканера, попробуйте считать штрих-коды с демонстрационных листов. Выясните, какие штрих-коды считываются, а какие нет.
3) Используя программу генерации штрих-кодов, сгенерируйте любой штрих-код, который сканер может считывать.
4) Попробуйте считать с экрана или при наличии принтера распечатайте его и отсканируйте.
5) О результатах работы сообщите преподавателю.

2. Построение системы контроля управлением доступом (СКУД) на базе контактных смарт-карт.

Цель работы

Ознакомиться с программированием контактных смарт-карт и построением СКУД на базе контактных смарт-карт.

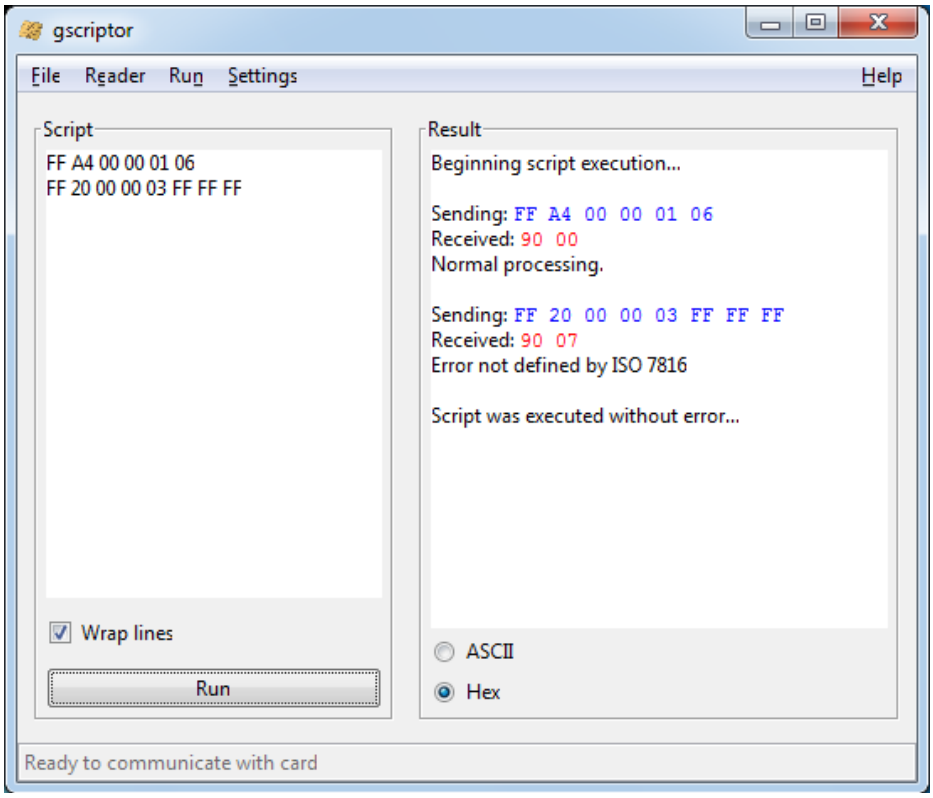
Учебный материал

2. Смарт-карты

2.1. Управление контактными смарт-картами.

Для управления контактными смарт-картами используйте APDU команды, описанные в стандарте ISO/IEC 7816.

Для отправки APDU команд используется программа G Scriptor. Ниже показан еѐ пример использования.



Карта памяти SLE5542

Карта памяти объѐмом 256 байт, где первые 32 байта могут быть защищены от записи, а так же необратимо записаны. Доступ к защищѐнной памяти осуществляется через 3 байтовый PIN-код. Количество попыток ввода PIN-кода 3 раза.

ADPU команды SLE5542

Выбор типа карты:

Включает и выключает карту в считывателе.

Формат посылаемых данных:

CLA=FF

INS=A4

P1=00

P2= 00

P3= 01

CardType=06

Формат получаемых данных:

SW1,SW2 если нет ошибок, то 90,00.

Чтение памяти карты:
Формат посылаемых данных:
CLA=FF
INS=B0
P1=00
P2= Адрес байта (от 00 до FF)
P3= Количество считываемых байтов
Формат получаемых данных:
BYTE1=прочитанный байт
…
BYTEn
SW1,SW2 - если нет ошибок, то 90,00.

Предоставить карте PIN-код:
Используется для проверки секретного кода, чтобы получить возможность записывать данные на карту.
Формат посылаемых данных:
CLA=FF
INS=20
P1=00
P2= 00
P3= 03
BYTE1= первый байт PIN-кода
BYTE2= второй байт PIN-кода
BYTE3=третий байт PIN-кода.
Формат получаемых данных:
SW1 - 90 если без ошибок.
SW2 — счѐтчик ошибок. 07 означает правильный код. 0 - карта заблокирована. 3 — осталось две попытки. 1 — осталось одна попытка.

Получить значение счѐтчика:
Формат посылаемых данных:
CLA=FF
INS=B1
P1=00
P2= 00
P3= 04
Формат получаемых данных:
ERRCNT - счѐтчик ошибок
DUMMY1, DUMMY2, DUMMY3, DUMMY4 - четыре случайных байта.
SW1,SW2 - если нет ошибок, то 90,00.
Чтение битов защиты:
Получение битов защиты для первых 32 байтов.
CLA=FF
INS=B2
P1=00
P2= 00
P3= 04
Формат получаемых данных:
PROT1, PROT2, PROT3, PROT4 - байты содержащие биты защиты.
SW1,SW2 - если нет ошибок, то 90,00.
Распределение битов защиты:

PROTO1
PROTO2
0 P8
0 P7
0 P6
0 P5
0 P4
0 P3
0 P2
0 P1
…
PX – бит защиты байта X, где «0» - запись запрещена, «1» - запись разрешена.
Запись в память карты:
Формат посылаемых данных:
CLA=FF
INS=D0
P1=00
P2= Адрес байта (от 00 до FF)
P3= Количество записываемых байтов
BYTE1=записываемый байт
…
BYTEn
Формат получаемых данных:
SW1,SW2 - если нет ошибок, то 90,00.
Запись в защищѐнную память карты:
Каждый байт сравнивается с байтом в памяти. Если они совпадают, то бит защиты для данно-го байта памяти необратимо программируется в «0».
Изменить PIN-код:
Изменяет текущий PIN-код карты. Доступна только после предоставления корректного PIN-кода.
Формат посылаемых данных:
CLA=FF
INS=D2
P1=00
P2= 01
P3= 03
BYTE1= первый байт PIN-кода
BYTE2= второй байт PIN-кода
BYTE3=третий байт PIN-кода.
Формат получаемых данных:
SW1,SW2 - если нет ошибок, то 90,00.

Ход работы

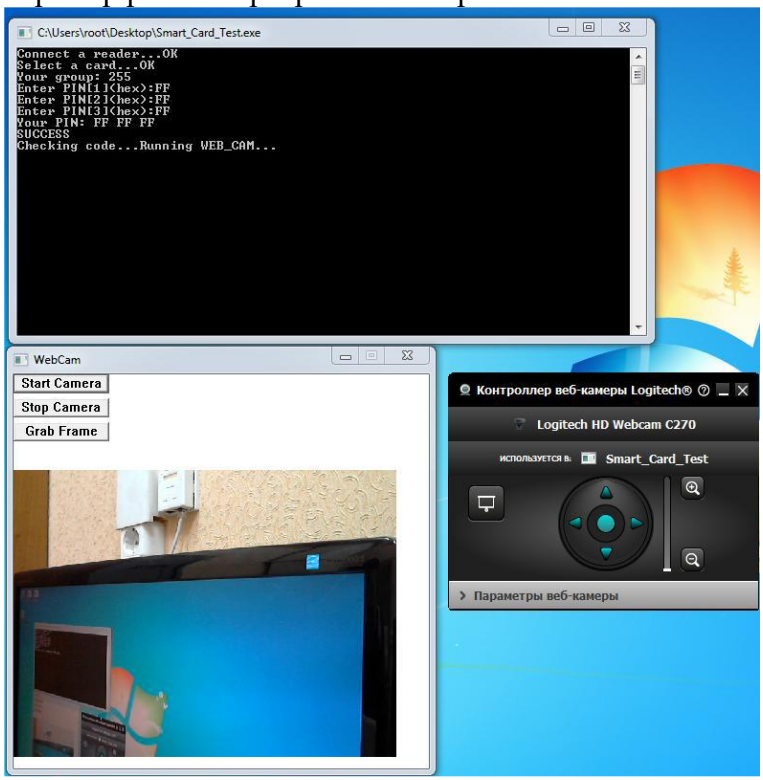
Внимание после 3 трѐх неверных попыток ввода PIN-кода карта безвозвратно блокируется.
1) Изучите APDU команды для смарт-карты SLE5542.
2) Используя программу G Scriptor, подключитесь к смарт-карте и введите PIN-код (по умолчанию FF FF FF).
3) Запишите в байт по адресу 0x20 число состоящие из двух младших цифр вашей группы.
4) Измените PIN-код карты.
5) Запишите в байт по адресу 0x09 значение 0xC7.

6) Запустите программу Smart Card Test. Убедитесь, что программа показывает число, введѐнное в пункте 3.

Введите PIN-код. После успешного ввода PIN-кода запустится веб-камера.

Покажите результат работы программы преподавателю.

Пример работы программы изображѐн ниже.



7) Измените PIN-код карты в исходное состояние.