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

Рассмотрено
цикловой комиссией
Протокол заседания № 1
от «31» августа 2020 г.
Председатель цикловой комиссии
_____/ Чобану Л.А./

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
профессионального модуля
ПМ 03. Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

по специальности
11.02.10 Радиосвязь, радиовещание, телевидение (углубленной подготовки)
квалификация
специалист по телекоммуникациям

Разработчик:
преподаватель
ОГАПОУ «Белгородский
индустриальный колледж»
Чобану Л.А.

Белгород 2020 г.

Содержание

1. Пояснительная записка

1.1. Краткая характеристика профессионального модуля, ее цели и задачи. Место лабораторных работ в курсе профессионального модуля

Профессиональный модуль ПМ 03. Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания является частью рабочей основной образовательной программы в соответствии с ФГОС по специальности СПО 11.02.10 Радиосвязь, радиовещание, телевидение (углубленной подготовки)

Профессиональный модуль изучается в IX семестре. В целом рабочей программой предусмотрено 52 часа на выполнения лабораторных работ, что составляет 40 % от обязательной аудиторной нагрузки, которая составляет 130 часа, при этом максимальная нагрузка составляет 195 часов, из них 65 часов приходится на самостоятельную работу обучающихся.

Цель настоящих методических рекомендаций: оказание помощи обучающимся в выполнении лабораторных работ по дисциплине ПМ 03. Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания, качественное выполнение которых поможет обучающимся освоить обязательный минимум содержания профессионального модуля и подготовиться к промежуточной аттестации в форме квалификационного экзамена.

1.2. Организация и порядок проведения лабораторных работ

Лабораторные работы проводятся после изучения теоретического материала. Введение лабораторных работ в учебный процесс служит связующим звеном между теорией и практикой. Они необходимы для закрепления теоретических знаний, а также для получения практических навыков и умений. При проведении лабораторных работ задания, выполняются студентом самостоятельно, с применением знаний и умений, усвоенных на предыдущих занятиях, а также с использованием необходимых пояснений, полученных от преподавателя. Обучающиеся должны иметь методические рекомендации по выполнению лабораторных работ, конспекты лекций, измерительные и чертежные инструменты, средство для вычислений.

1.3. Общие указания по выполнению лабораторных работ

Курс лабораторных работ по дисциплине ПМ 03. Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания предусматривает проведение 26 работ, посвященных изучению:

- выявлению различных каналов утечки информации;
- исследованию методов и средств защиты информации;
- мониторингу сетевого трафика;
- установке и настройке различных по защите информации;
- криптографическим исследованиям.

При подготовке к проведению лабораторной работы необходимо:

• ознакомиться с лабораторным оборудованием;

• ознакомиться с порядком выполнения работы

После выполнения лабораторной работы обучающийся к следующему занятию оформляет отчет, который должен содержать:

• название лабораторной работы, ее цель;

• краткие, общие сведения об изучаемом лабораторном оборудовании;

• необходимый графический материал, указанный преподавателем при выполнении лабораторной работы (принципиальная схема лабораторной установки, графики);

• данные, полученные непосредственно из проводимых опытов;

• результаты обработки данных опытов с необходимыми пояснениями;

• графический материал, отображающий полученные в ходе опытов значения измеряемых величин;

• оценку результатов испытаний.

При работе в лаборатории необходимо руководствоваться инструкциями по технике безопасности, учитывающими все специфические особенности лаборатории.

В лаборатории нельзя находиться в отсутствие преподавателя или лица, ответственного за технику безопасности.

При нахождении в лаборатории следует находиться в рабочей зоне, указанной преподавателем. С самого начала необходимо убедиться в том, что испытательный стенд находится в полностью обесточенном (отключенном) состоянии.

Перед выполнением лабораторной работы необходимо получить вводные инструкции преподавателя и внимательно ознакомиться с описанием лабораторного стенда и оборудованием.

Внимание! Включать лабораторные установки и выполнять какие-либо действия с приборами допускается ТОЛЬКО с разрешения преподавателя!

При обнаружении признаков неисправности, таких как: появление искрения, дыма, специфического запаха, следует немедленно отключить все источники электроэнергии и сообщить о случившемся преподавателю.

При возникновении реальной опасности травматизма для одного или нескольких присутствующих, участники испытания должны произвести срочное отключение лаборатории от всех источников электроэнергии выключением вводного автомата. Лаборатории должны иметь средства пожаротушения и оказания первой медицинской помощи. На первом занятии изучаются правила техники безопасности и проводится вводный инструктаж с последующей проверкой его усвоения, о чем свидетельствует запись в журнале по технике безопасности кабинета/лаборатории, подписываемый преподавателем, проводившем инструктаж, и всеми обучающимися.

1.4. Критерии оценки результатов выполнения лабораторных работ

Критериями оценки результатов работы обучающихся являются:

– уровень усвоения обучающимся учебного материала;

– умение обучающегося использовать теоретические знания при выполнении практических задач;

– сформированность общеучебных и профессиональных компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.

ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.

ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Быть готовым к смене технологий в профессиональной деятельности.

В результате освоения дисциплины обучающийся должен обладать профессиональными компетенциями, соответствующими видам деятельности:

ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.

ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование сетей вещания.

- обоснованность и четкость изложения материала;
- уровень оформления работы.
- анализ результатов.

Критерии оценивания лабораторной работы

Оценка	**Критерии оценивания**
5	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, формулирует собственные, самостоятельные, обоснованные, представляет полные и развернутые ответы на дополнительные вопросы.
4	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, допуская незначительные ошибки на дополнительные вопросы.
3	Работа выполнена в полном объеме, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, допуская ошибки на дополнительные вопросы.
2	Работа выполнена не полностью. Студент практически не владеет теоретическим материалом, допускает ошибки при ответе на дополнительные вопросы.

2. Тематическое планирование лабораторных работ

	Наименование тем	Вид и название работы студента	Количество часов на выполнение работы
Раздел 1	**Ведение комплексной системы защиты информации в телекоммуникационных системах и сетях вещания**		**52**
1.2	**Методы и способы защиты информации**	**Лабораторная работа №1 «**Выявление каналов утечки информации»	2
		Лабораторная работа №2 «Подтверждение и проверка аутентичности и целостности информации.»	2
		Лабораторная работа №3 «Защита от несанкционированного доступа к информации»	2
		Лабораторная работа №4 «Разграничение доступа.»	2
		Лабораторная работа №5 «Создание резервных копий.»	2
		Лабораторная работа №6 «Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ»	2
		Лабораторная работа №7 «Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем.»	2
		Лабораторная работа №8 «Изучение принципов идентификации и механизмов подтверждения подлинности пользователя. Правила формирования электронной цифровой подписи»	2
		Лабораторная работа №9 «Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.»	2
		Лабораторная работа №10 «Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия.»	2
		Лабораторная работа №11 «Реализация информационных технологий для построения защищенной	2

		информационно-вычислительной сети»	
		Лабораторная работа №12 «Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы, исходящие от использования «электронной почты».»	2
1.3	**Защита информации в системах радиосвязи и сетях вещания**	**Лабораторная работа №13 «**Исследование методов тестирования и контроля защищенных систем радиосвязи»	2
		Лабораторная работа №14 «Исследование методов защиты телетрафика в сетях и систем радиосвязи»	2
		Лабораторная работа №15 «Методы и средства защиты телефонных линий»	2
		Лабораторная работа №16 «Мониторинг и диагностика средств защиты беспроводной локальной сети стандарта IEEE 802.11»	2
		Лабораторная работа №17 «Исследование методов цифровой обработки сигналов на основе сигнальных процессоров в защищенных системах радиосвязи»	2
2.1.	**Основные направления защиты информации**	**Лабораторная работа №18 «**Установка и настройка оборудования по защите информации»	2
		Лабораторная работа №19 «Обнаружение «радио-жучков»»	2
		Лабораторная работа №20 «Изучение принципа работы детектора поля.»	2
		Лабораторная работа №21 «Установка и настройка программных средств защиты информации»	2
2.2.	**Системы условного доступа в сетях вещания**	**Лабораторная работа №22-23 «**Система условного доступа Conax»	4
		Лабораторная работа №24-26 «Система условного доступаIP CAS / DRM.»	6
		Итого:	**52**

3. Содержание лабораторных работ

ЛАБОРАТОРНАЯ РАБОТА№1
ТЕМА:ВЫЯВЛЕНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ
Цель: Изучить технические средства утечки информации.

Безопасных технических средств передачи информации нет. Источниками образования технических каналов утечки информации являются физические преобразователи. Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации. Любой канал утечки информации может быть обнаружен и локализован. "На каждый яд есть противоядие". Канал утечки информации легче локализовать, чем обнаружить.

Под техническим каналом утечки информации (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.

Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими, и т. д. То есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах.

В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. Например, воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт (земля) и т. п.

Любая система связи (система передачи информации) состоит из источника информации, передатчика, канала передачи информации, приемника и получателя сведений. Эти системы используются в повседневной практике в соответствии со своим предназначением и являются официальными средствами передачи информации, работа которых контролируется с целью обеспечения надежной, достоверной и безопасной передачи информации, исключающей неправомерный доступ к ней со стороны конкурентов. Однако существуют определенные условия, при которых возможно образование системы передачи информации из одной точки в другую независимо от желания объекта и источника. При этом, естественно, такой канал в явном виде не должен себя проявлять. По аналогии с каналом передачи информации такой канал называют каналом утечки информации. Он также состоит из источника сигнала, физической среды его распространения и приемной аппаратуры на стороне злоумышленника. Движение информации в таком канале осуществляется только в одну сторону — от источника к злоумышленнику. На рисунке приведена структура канала утечки информации.

Структура канала утечки информации

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведении.

Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике **с учетом физической природы образования каналы утечки информации** можно квалифицировать на следующие **группы**:

1. технические каналы утечки информации при ее передачи по каналам связи;
2. технические каналы утечки речевой информации;
3. технические каналы утечки информации обрабатываемой ТСПИ;
4. технические каналы утечки видовой информации.

КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ ОБРАБАТЫВАЕМОЙ ТСПИ

Электромагнитные каналы утечки информации. К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ЭМИ) ТСПИ:

- излучений элементов ТСПИ;
- излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ;
- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Зона, в которой возможны перехват (с помощью разведывательного приемника) побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации (т.е. зона, в пределах которой отношение "информационный сигнал/помеха" превышает допустимое нормированное значение), называется (опасной) зоной.

Электрические каналы утечки информация. Причинами возникновения электрических каналов утечки информации могут быть [8,17,40]:

- наводки электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;
- просачивание информационных сигналов в цепи электропитания ТСПИ;
- просачивание информационных сигналов в цепи заземления ТСПИ.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к системам электропитания и заземления ТСПИ. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Электронные устройства перехвата информации, устанавливаемые в ТСПИ, часто называют **аппаратными закладками.** Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в ТСПИ иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал утечки информации. Перехват обрабатываемой в технических средствах информации возможен также путем их "высокочастотного облучения".

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ АКУСТИЧЕСКОЙ (РЕЧЕВОЙ) ИНФОРМАЦИИ

Под акустической понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.

В воздушных (прямых акустических) технических каналах утечки информациисредой распространения акустических сигналов является воздух. Для перехвата акустических сигналов в качестве датчиков средств разведки используются микрофоны. Сигналы, поступающие с

микрофонов или непосредственно, записываются на специальные портативные устройства звукозаписи или передаются с использованием специальных передатчиков в пункт приема, где осуществляется их запись.

Для перехвата акустической (речевой) информации используются:

– портативные диктофоны и проводные микрофонные системы скрытой звукозаписи;

– направленные микрофоны;

– акустические радиозакладки (передача информации по радиоканалу);

– акустические сетевые закладки (передача информации по сети электропитания 220В);

– акустические ИК-закладки (передача информации по оптическому каналу в ИК-диапазоне длин волн);

– акустические телефонные закладки (передача информации по телефонной линии на высокой частоте);

– акустические телефонные закладки типа “телефонное ухо” (передача информации по телефонной линии “телефону-наблюдателю” на низкой частоте).

В виброакустических технических каналах утечки информациисредой распространения акустических сигналов являются ограждения конструкций зданий, сооружений (стены, потолки, полы), трубы водоснабжения, канализации и другие твердые тела.

Для перехвата акустических колебаний в этом случае используются средства разведки с контактными микрофонами:

– электронные стетоскопы;

– радиостетоскопы (передача информации по радиоканалу).

Оптико-электронный (лазерный) канал утечкиакустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.). Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы, иногда называемые **“лазерными микрофонами”.**

Электроакустические технические каналы утечки информации. Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих "микрофонным эффектом", а также путем "высокочастотного навязывания".

Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. Для исключения воздействия высокочастотного сигнала на аппаратуру АТС в линию, идущую в ее сторону, устанавливается специальный высокочастотный фильтр.

Параметрические технические каналы утечки информации. Параметрический канал утечки информации может быть реализован и путем "высокочастотного облучения" помещения, где установлены полуактивные закладные устройства, имеющие элементы, некоторые параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются по закону изменения акустического (речевого) сигнала.

Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленным излучением и приемник.

КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА ТЕХНИЧЕСКИХ КАНАЛОВ ПЕРЕХВАТА ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ

Информация после обработки в ТСПИ может передаваться по каналам связи, где также возможен ее перехват.

Электромагнитный канал перехвата информации. 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.

Электрический канал перехвата информации. Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.

Самый простой способ - это непосредственное параллельное подключение к линии связи. Но данный факт легко обнаруживается, так как приводит к изменению характеристик линии связи за счет падения напряжения.

Индукционный канал перехвата информации. В случае использования сигнальных устройств контроля целостности линии связи, ее активного и реактивного сопротивления факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индуктивный канал перехвата информации, не требующий контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики используются в основном для съема информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Современные индукционные датчики способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами.

КЛАССИФИКАЦИЯ И ХАРАКТЕРИСТИКА СПОСОБОВ СКРЫТОГО ВИДЕОНАБЛЮДЕНИЯ И СЪЕМКИ

Наряду с информацией, обрабатываемой в ТСПИ, и акустической (речевой) информацией, важную роль играет видовая информация, получаемая техническими средствами разведки в виде изображений объектов или документов.

В зависимости от характера информации и ее предназначения можно выделить следующие способы ее получения:

- наблюдение за объектом;
- съемка объекта;
- съемка (снятие копий) документов.

Наблюдение за объектом. Наблюдение за объектом организуется в течение определенного (в ряде случаев длительного) времени.

В зависимости от условий наблюдения и освещения для наблюдения за объектом могут использоваться различные технические средства. Для наблюдения днем - оптические приборы (монокуляры, подзорные трубы, бинокли, телескопы и т.д.), телевизионные камеры (системы), для наблюдения ночью - приборы ночного видения, телевизионные камеры (системы), тепловизоры.

Для наблюдения с большого расстояния используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния - камуфлированные скрытно установленные телевизионные камеры. Причем видеоизображение с телевизионных камер может передаваться на мониторы, как по кабелю, так и по радиоканалу.

Съемка объектов. Съемка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов.

Причем фотоаппараты используются в случае, когда необходимо получить отдельные изображения, например, внешний вид объекта или фотоснимок сотрудника, а телевизионные - когда необходимо получить изображения динамического процесса, например технологического цикла, или действий отдельных лиц.

Съемка объектов ночью проводится, как правило, с близкого расстояния. Для этих целей используются портативные фотоаппараты и телевизионные камеры, комплексированные с приборами ночного видения, или тепловизоры, а также портативные закамуфлированные

телевизионные камеры высокой чувствительности, комплексированные с устройствами передачи информации по радиоканалу.

ЛАБОРАТОРНАЯ РАБОТА№2
ТЕМА: ПОДТВЕРЖДЕНИЕ И ПРОВЕРКА АУТЕНТИЧНОСТИ И ЦЕЛОСТНОСТИ ИНФОРМАЦИИ
ЦЕЛЬ: НАУЧИТЬСЯ ПРИМЕНЯТЬ СТАНДАРТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В MSOFFICE

Чтобы защитить документ в MicrosoftWord, следует воспользоваться опциями на закладке **Защита документа (Security)** в диалоговом окне **Рецензирование (Options)**.В этом диалоговом окне можно установить пароль, который должен быть введен прежде, чем кто-то сможет открыть или изменить документ. Выбор флажка “Рекомендовать доступ только для чтения” (Read-onlyrecommended) позволяет отображать сообщение, которое рекомендует пользователю открывать документ только для чтения. Можно также использовать кнопку “Установить защиту” (ProtectDocument) на закладке Безопасность (Security), чтобы установить пароли, для ограничения, кто может вносить изменения или вводить комментарии.

Можно так же использовать кнопку «Установить защиту» на вкладке **Безопасность,** чтобы установить пароль для ограничения круга лиц кто может вносить изменения или вводить комментарии. Аналогичные ограничения можно установить с помощью команды **Рецензирование – Защита документов**. Здесь можно устанавливать ограничения на использование стилей форматирования документов, а так же разрешить или запретить некоторым пользователям способы редактирования документов. Для подтверждения защиты необходимо нажать кнопку «Да, включить защиту».

MicrosoftExcel поддерживает три уровня защиты при сохранении книг. Эти параметры могут использоваться как вместе, так и по отдельности:

Пароль для открытия (Passwordtoopen): для того чтобы открыть книгу, пользователь должен ввести пароль, являющийся кодом, с помощью которого был зашифрован файл.

Пароль для изменения (Passwordtomodify): для того чтобы открыть книгу в режиме редактирования, пользователь должен ввести пароль. Не вводя пароль, пользователь может открыть книгу в режиме только для чтения.

Рекомендовать доступ только для чтения (Read-onlyrecommended): пользователю предлагается открыть документ в режиме только для чтения. Если в диалоговом окне пользователь нажимает кнопку Нет (No), а какой-либо другой метод защиты не используется, книга Excel открывается в режиме редактирования.

Для шифрования книг используются различные криптографические методы, которые можно выбрать, нажав кнопку Дополнительно (Advanced) в диалоговом окне Параметры сохранения (SaveOptions), доступном из меню Файл - Сохранить как - Сервис - Общие параметры (File - SaveAs - Tools - GeneralOptions). Метод шифрования по умолчанию можно также задать с помощью системных политик. В дополнение к защите всей книги MicrosoftExcel Вы также можете защитить от несанкционированных изменений отдельные области этой книги.

В некоторой степени можно защитить книгу с помощью следующих параметров, доступных в меню Рецензирование - Защитить лист

Задание

Создайте на диске С в папке Temp файл MicrosoftWord и MicrosoftExcel.

1. Произвести защиту созданного вами документа MicrosoftWord от несанкционированного прочтения и внесения изменений. Установить ограничения на редактирование документа и разрешить **Ввод данных в поля формы**. Просмотреть, какой результат дает это ограничение. Завершить работу с Word.

2. Произвести защиту книги и листа документа MicrosoftExcel. от несанкционированного прочтения и внесения изменений. Установить ограничения на форматирование ячеек таблицы, вставку и удаление столбцов и строк. Завершить работу с Excel.

ЛАБОРАТОРНАЯ РАБОТА №3
ТЕМА: ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Как показывает практика, несанкционированный доступ (НСД)представляет одну из наиболее серьезных угроз для злоумышленного завладения защищаемой информацией всовременных АСОД.Как ни покажется странным, но для ПК опасность данной угрозы по сравнению сбольшими ЭВМповышается, чему способствуют следующие объективно существующие обстоятельства:

1) подавляющая часть ПКрасполагается непосредственно врабочих комнатах специалистов, что создает благоприятные условия для доступа кним посторонних лиц;

2) многие ПКслужат коллективным средством обработки информации, что обезличивает ответственность, втом числе изазашить информации;

3) современные ПКоснащены несъемныминакопителями на ЖМДочень большой емкости, причем информация на них сохраняется даже вобесточенном состоянии;

4)накопителина ГМД.производятся втаком массовом количестве,,что уже используются для распространения информациитак же как и бумажные носители;

5) первоначальноПКсоздавались именно как персональное средство автоматизации обработки информации, апотому ине оснащались специальносредствами защиты от НСД.

В силу сказанного те пользователи, которые желают сохранить конфиденциальность своей информации, должны особенно позаботиться обоснащении используемой ПКвысокоэффективными средствами защиты от НДС.

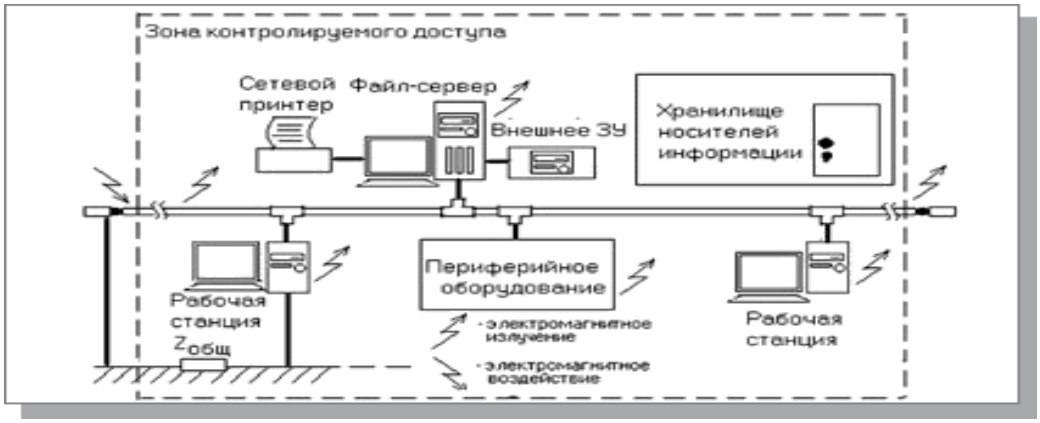


Рисунок . Места и каналы возможного несанкционированного доступа (НСД).

Основные механизмы защиты ПКот НСДмогут быть представленыследующим перечнем:

1) физическая зашита ПКиносителей информации;

2) опознавание (ааутентификация)пользователей ииспользуемых компонентов обработки информации;

3) разграничение доступа кэлементам защищаемой информации;

4) криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);

5) криптографическое закрытие защищаемой информации в ппроцессенепосредственной ее обработки;

6) регистрация всех обращений кзащищаемой информации.

Новое решение компании HID Global — ActivIdentityCardManagementSystem (CMS) предназначено для создания высокозащищенных систем ограничения доступа к компьютерам, корпоративным сетям и приложениям, а также контроля доступа в помещения на предприятиях с численностью до 10 000 сотрудников. CMS совместима с различными операционными системами, системами управления идентификационными данными и СКУД, поэтому быстро интегрируется в существующую IT-инфраструктуру с помощью сервера ActivIdentity 4TRESS AAA, поддерживающего LDAP-каталоги и базы данных SQL-типа. При этом защита компьютера от несанкционированного доступа базируется на технологии открытых ключей PKI, а выполнение криптографических операций осуществляется с помощью USB-приемников, подключаемых к ПК пользователей, и смарт-карт HID.

Система ActiveIDentityCardManagementSystem (CMS) является эффективным и экономичным решением для ограничения физического и логического доступа (защиты компьютера) в крупных организациях, включая правительственные учреждения, офисы компаний и банковский сектор. ActiveIDentity CMS позволяет отойти от традиционных механизмов контроля доступа к ПК, базирующихся на идентификации пользователей по логину и паролю, и минимизирует проблемы управления большим и переменным числом конечных пользователей. Благодаря использованию такой системы обеспечивается достаточно высокая степень защиты компьютера от несанкционированного доступа, и ограничивается доступ к корпоративным данным.

Внедрение ActiveIDentity CMS малозатратно и с финансовой точки зрения и по времени: опытный инсталлятор способен установить и запустить систему защиты компьютера всего за 30 минут. Настройка системы и защита компьютера от несанкционированного доступа осуществляется с помощью специальных утилит, входящих в CardManagementSystem. Сочетание в системе логического и физического доступа также снижает ее стоимость владения и позволяет автоматизировать систему допуска к данным, что сегодня наиболее важно для больших предприятий. Вход в систему может осуществляться по смарт-картам ActiveIDentity, которые поддерживают широкий спектр технологий аутентификации пользователей: от входа в здание, до доступа к компьютеру, в сеть и различные приложения.

Совместимость программно-аппаратного комплекса ActivIdentity с большим числом ИТ-приложений позволяет развернуть систему на базе уже внедренных на объекте технологий. Для защиты компьютера и информации поддерживается большое число директорий, удостоверяющих центров, включая Microsoft CA, OpenTrust PKI и др., а также систем контроля доступа компаний Lenel, Honeywell, Tyco и др., систем электронных платежей, различных типов смарт-карт и баз данных. С помощью CMS возможна организация логического доступа и защита компьютера от несанкционированного доступа путем ее интеграции в уже существующую IT-среду предприятия с помощью сервера ActivIdentity 4TRESS AAA.

Комплексная защита компьютера и данных будет выполнена наиболее эффективной при активации приложения ActivIdentity CMS Appliance, использующего технологии аутентификации с помощью открытых ключей (PKI). Это приложение представляет собой систему, связывающую открытые ключи шифрования с личностью пользователя посредством удостоверяющего центра (УЦ). В отличие от решений на платформе NaviGo, защита компьютера от несанкционированного доступа с помощью CMS Appliance обеспечивается на более высоком уровне, а также поддерживается работа с различными приложениями, в числе которых электронный кошелек, оплата проезда и т.д.

ЛАБОРАТОРНАЯ РАБОТА №4
ТЕМА: РАЗГРАНИЧЕНИЕ ПРАВ ДОСТУПА.
ЦЕЛЬ: ИЗУЧИТЬ ОСНОВНЫЕ ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. НАУЧИТСЯ УПРАВЛЯТЬ ДОСТУПОМ К ЭЛЕМЕНТАМ СИСТЕМЫ.

Шифрование и дешифрование файлов и папок

Шифрование файлов и папок. Поскольку шифрование и дешифрование выполняется автоматически, пользователь может работать с файлом так же, как и до установки его криптозащиты. Например, можно так же открыть текстовый процессор Word, загрузить документ и отредактировать его, как и прежде. Все остальные пользователи, которые попытаются получить доступ к зашифрованному файлу, получат сообщение об ошибке доступа, поскольку они не владеют необходимым личным ключом, позволяющим им расшифровать файл.

Следует отметить, что пользователи (в данном случае администраторы) не должны шифровать файлы, находящиеся в системном каталоге, поскольку они необходимы для загрузки системы, в процессе которой ключи пользователя недоступны. Это сделает невозможным дешифрование загрузочных файлов, и система потеряет работоспособность. Проводник предотвращает возможность возникновения такой ситуации, не позволяя шифровать файлы с атрибутом *системный.*

Дешифрование файлов и папок. Чтобы дешифровать файл или папку, на вкладке Общие окна свойств соответствующего объекта нажмите кнопку Другие.

В открывшемся окне диалога в группе Атрибуты сжатия и шифрования сбросьте флажокШифровать содержимое для защиты данных.

Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок. Операции копирования, перемещения, переименования и уничтожения зашифрованных файлов и папок выполняются точно так же, как и с незашифрованными объектами. Однако следует помнить, что пункт назначения зашифрованной информации должен поддерживать шифрование. В противном случае при копировании данные будут расшифрованы, и копия будет содержать открытую информацию.

Архивация зашифрованных файлов. Резервную копию зашифрованного файла можно создать с помощью простого копирования его на другой жесткий диск или с использованием утилиты архивации. Однако, как сказано в предыдущем пункте, простое копирование, например, на дискету или оптический диск может привести к тому, что резервная копия будет содержать открытые данные. То есть, если скопировать зашифрованный файл на раздел FAT или на дискету, копия будет не зашифрована и, следовательно, доступна для чтения любому пользователю. Специализированная операция архивации не требует для ее выполнения доступа к открытым ключам пользователя - только к архивируемой информации. Поэтому для обеспечения безопасности конфиденциальных данных при создании резервных копий рекомендуется применять специальные утилиты архивации. В Windows для этих целей предназначена стандартная утилита архивации данных Backup.

Задание 1.

Шифрование информации задается в окне свойств файла или папки: Создайте на диске С в папке Temp папку со своим именем и проделайте следующие действия для ее шифрования:

1. Укажите файл или папку, которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду Свойства.
2. В появившемся окне свойств на вкладке Общие нажмите кнопку Другие. Появится окно диалога Дополнительные атрибуты (рис. 1).
3. В группе Атрибуты сжатия и шифрования установите флажокШифровать содержимое для зашиты данных и нажмите кнопку ОК.
4. Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки. В появившемся окне диалога укажите режим шифрования.

При шифровании папки можно указать следующие режимы применения нового атрибута:

- Только к этой папке

- К этой папке и всем вложенным папкам и файлам

Сведения об особенностях управления доступом к папкам и файлам (общих правах доступа, полном наборе прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта).

Разграничение прав доступа осуществляется с использованием команды «Общий доступ и безопасность». Если данная команда недоступна (при работе в ОС WindowsXPProfessional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки.

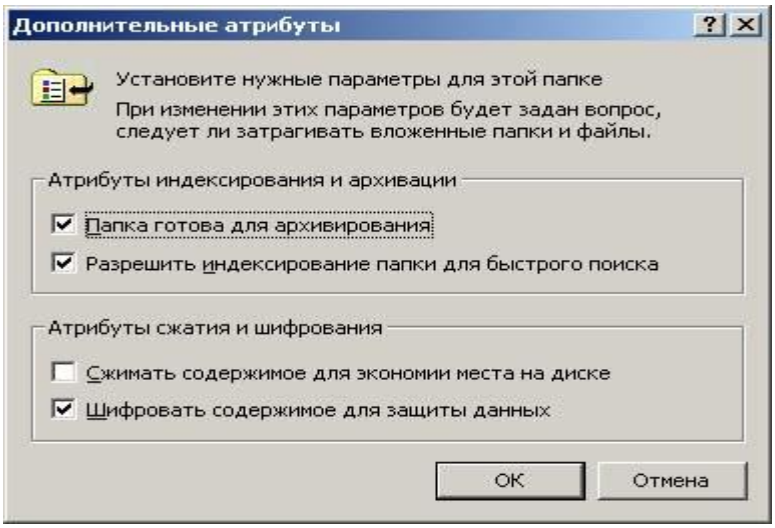


Рисунок 1. Окно диалога Дополнительные атрибуты

Разграничение прав доступа к файлам

Чтобы включить команду «Общий доступ и безопасность», используемую для управления общим доступом к папкам и файлам необходимо выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки.

Общие права доступа задаются во вкладке *Доступ* при просмотре свойств файла. Полный набор прав доступа для конкретного файла (папки) можно просмотреть: Свойства – вкладка *Безопасность* – *Дополнительно* – вкладка *Разрешения* – выбрать пользователя, начать кнопку*Изменить*. Появится окно с полным набором прав доступа.Текущего владельца данного объекта можно определить на вкладке *Владелец* свойств объекта. Действующие разрешения можно посмотреть на вкладке *Действующие* разрешения.

Сведения об особенностях управления доступом к принтерам и разделам реестра (общих правах доступа, полном наборе прав доступа, владельце объекта, действующих разрешениях на доступ к объекту для конкретного субъекта).

Общие права доступа к принтеру задаются во вкладке Доступ его свойств по аналогии с установлением прав доступа на файлы и папки.

Полный набор прав доступа к конкретному принтеру можно просмотреть: Свойства – вкладка *Безопасность* – *Дополнительно* – вкладка *Разрешения* – выбрать пользователя, начать кнопку*Изменить*. Появится окно с полным набором прав доступа, который существенно отличается от набора прав на файлы и папки.

Текущего владельца принтера можно определить на вкладке *Владелец* свойств принтера. Действующие разрешения можно посмотреть на вкладке *Действующие* разрешения.

Для управления доступом к разделу реестра мы должны зайти в редактор реестра, выделить нужный раздел в древовидной структуре, вызвать правой кнопкой контекстное меню и выбрать пункт «Разрешения». Для управления полным набором прав доступа в появившемся окне надо нажать кнопку дополнительно, затем выбрать вкладку Разрешения, нужного пользователя и просмотреть полный список разрешений.Здесь же во вкладке Владелец мы можем просмотреть владельца данного субъекта. Действующие разрешения на доступ к объекту для конкретного субъекта мы можем посмотреть тут же во вкладке Действующие разрешения.

Задание 2

1. Создайте на диске С в папке Temp файл с произвольным расширением.

2. Просмотрите свойства этого файла (нажать на файл правой кнопкой мыши и выбрать пункт контекстного меню Свойства).

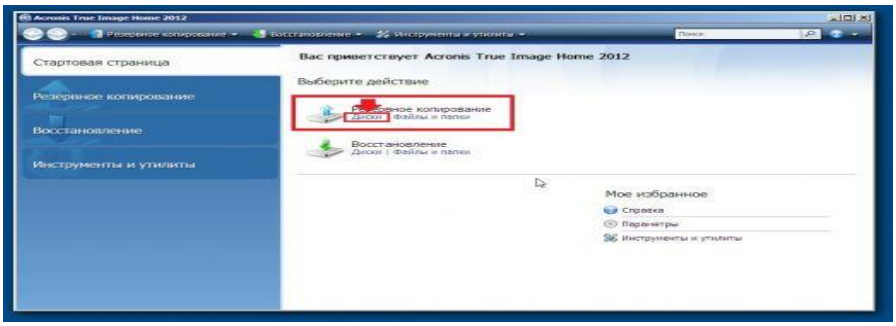
3. Ограничьте доступ к файлу на уровне чтения. Для этого сначала выделите пользователя, для которого вы ограничиваете доступ, установите нужные ограничения.

4. Полный набор прав доступа для конкретного файла (папки) можно просмотреть: Свойства – вкладка *Безопасность* – *Дополнительно* – вкладка *Разрешения* – выбрать пользователя, нажать кнопку*Изменить*. Появится диалоговое окно с полным набором прав доступа.

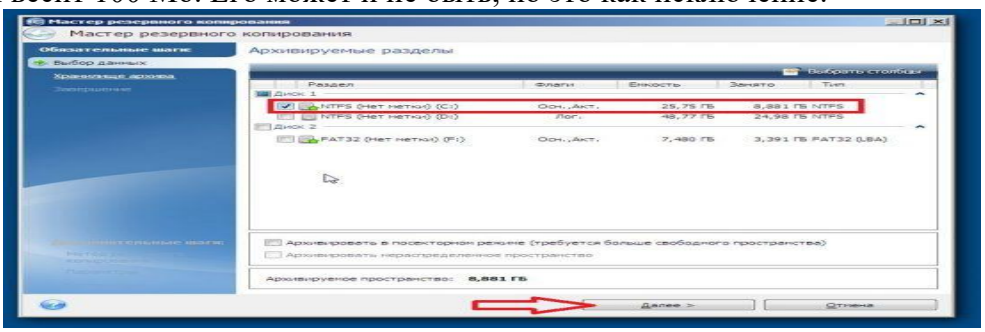
ЛАБОРАТОРНАЯ РАБОТА №5
ТЕМА: СОЗДАНИЕ РЕЗЕРВНЫХ КОПИЙ
ЦЕЛЬ: Как создать резервную копию Windows. Восстановление системы с программами и драйверами

Основное достоинство резервирования Windows с помощью создания **образа диска** с установленной системой и программами – это уверенность на 100%, что после того, как вы пере зальете Windows, все программы, установленные на момент создания копии системы, будут работать. Образ операционной системы можно записать на другой компьютер, но в этом случае придется переустанавливать все драйвера под новое железо.

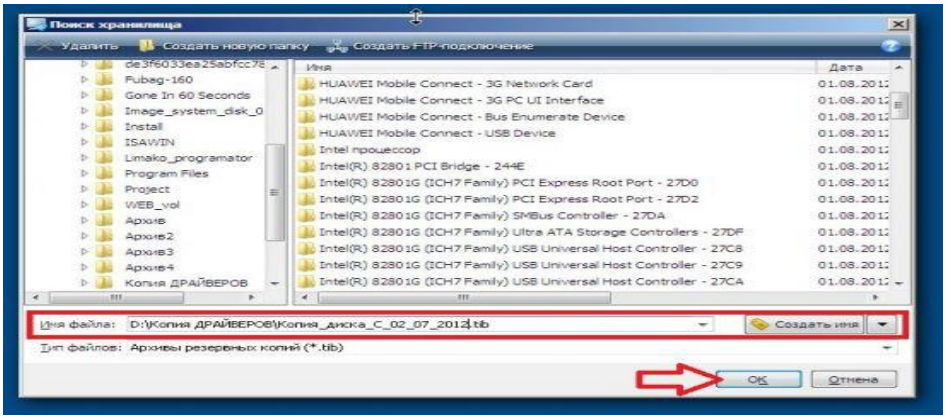
Как создать резервную копию Windows с помощью AcronisTrueImage. Делать резервную копию необходимо при помощи загрузочного диска или флешки. Лучшим инструментом для создания образа с Windows, по мнению многих системных администраторов, считается **AcronisTrueImage**. Прежде всего, перед началом основной работы по созданию копии диска с операционной системой, нужно **сделать загрузочную флешку с AcronisTrueImage**. Надеюсь, проблем с созданием флешки с Акронисом у вас не возникнет. На сайте так же описано, **как настроить БИОС под загрузку с флешки**. После успешной загрузки образа с Acronis TI вы увидите вот такое окно.



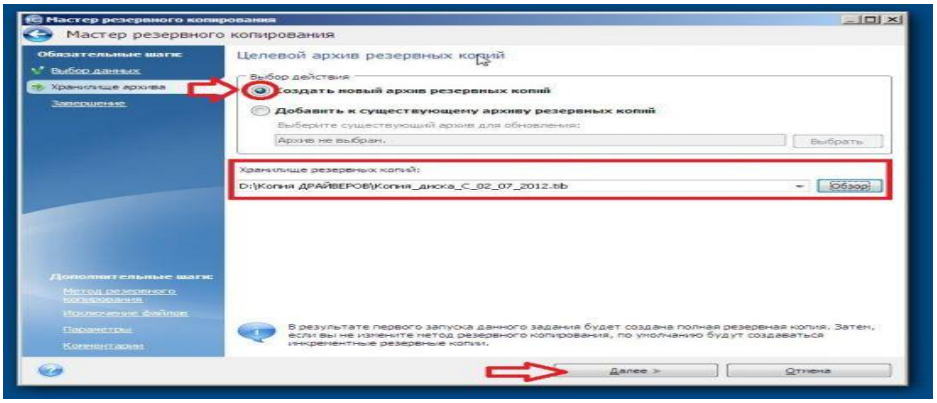
Нажимаем «Диски», так как мы создаем образ всего диска с **Windows**. И вот тут уже вступает в дело мастер **резервного копирования**. Обычно диск с операционной системой обозван как (C:), убедитесь в этом перед тем, как делать копию. Я рекомендую ориентироваться по размеру диска, тогда точно не ошибетесь. Окончательно убедившись, ставьте галку напротив системного диска. Если установлена Windows 7 (семерка), необходимо так же ставить галку напротив раздела, который весит 100 Мб. Его может и не быть, но это как исключение.



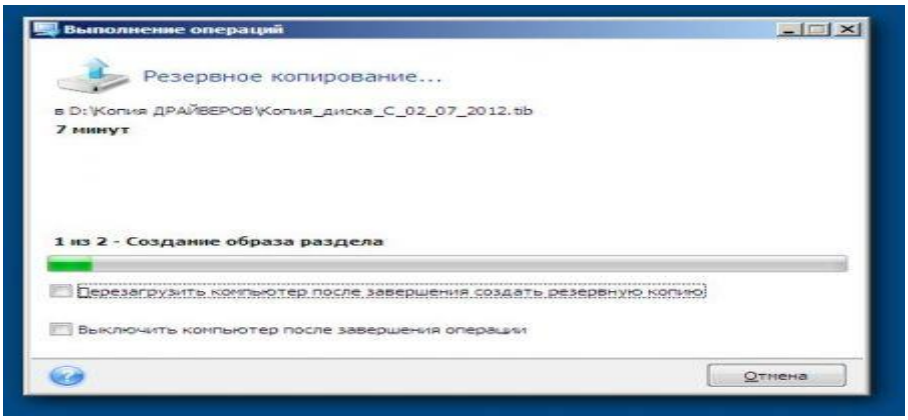
Теперь нужно выбрать место, куда будет записан архив. Сохранить копию можно куда угодно, на флешку, еще куда-то, НО ни в коем случае не на том же диске, который вы резервируете. Задаем архиву имя, чтобы потом было понятно, советую использовать в имени дату создания.



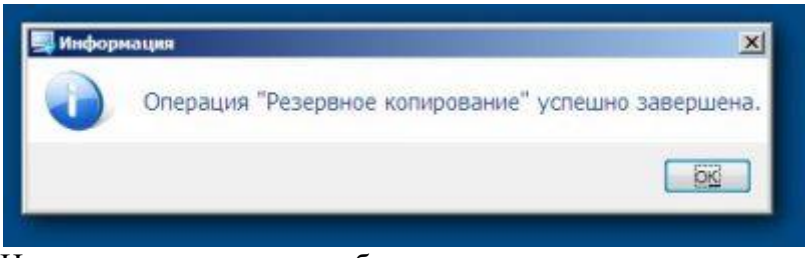
В следующем шаге ничего не меняем, только проверяем, правильно ли выбрали хранилище резервных копий.



И затем останется только нажать на кнопку «приступить» и наблюдать, как AcronisTrueImage производит резервирование вашей винды.



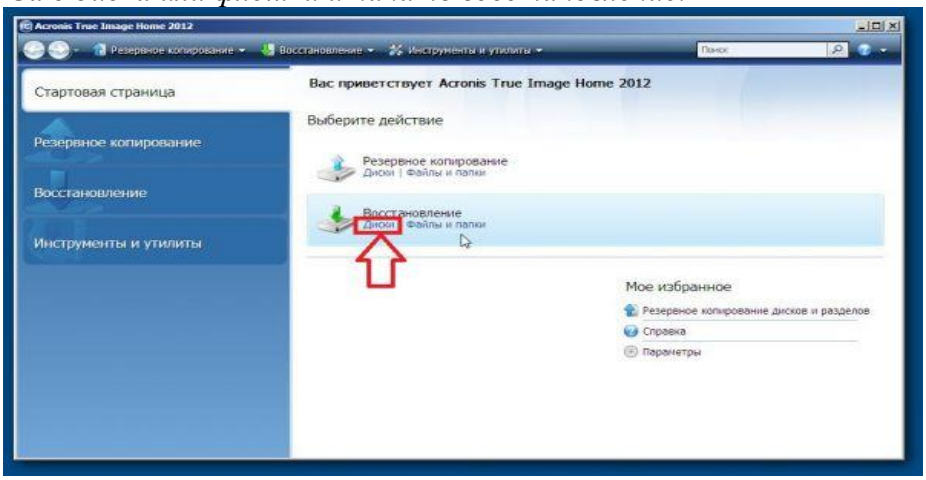
Минут 5-10 ждем, ничего не трогаем и вот оно, сообщение об успешном резервном копировании!



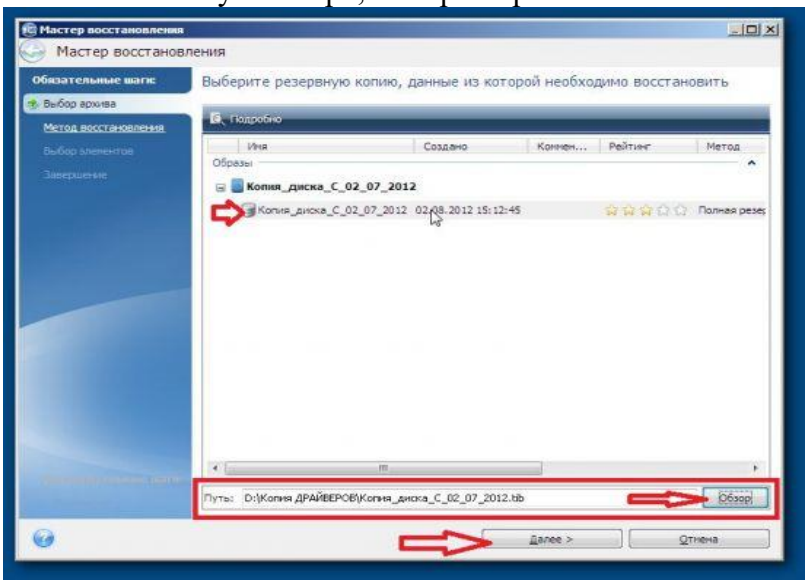
Ну, теперь главное не забыть, где размещена ваша резервная копия, которая включает в себя все программы, вами заранее установленные и драйвера.

Восстановление системы из резервной копии. *Чудесное воскрешение загнувшейся системы за считанные минуты, для подготовившегося пользователя это пустяк. И когда настанет момент, когда Windows уже не может нормально функционировать, этот прозорливый*

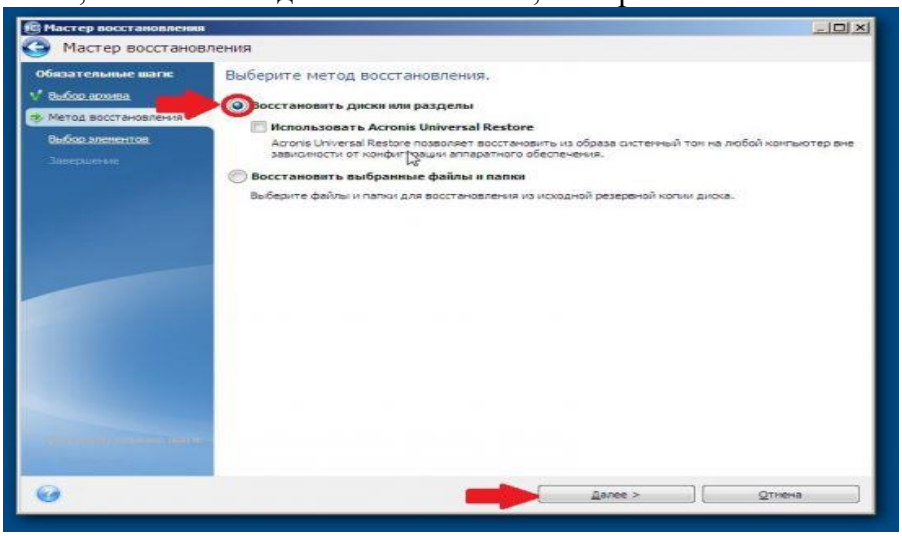
пользователь должен будет иметь под рукой загрузочный носитель с Акронис, а так же должен помнить, где находится резервная копия операционной системы. Опять же нужно загрузиться из под БИОСа с диска или флешки и начать восстановление.



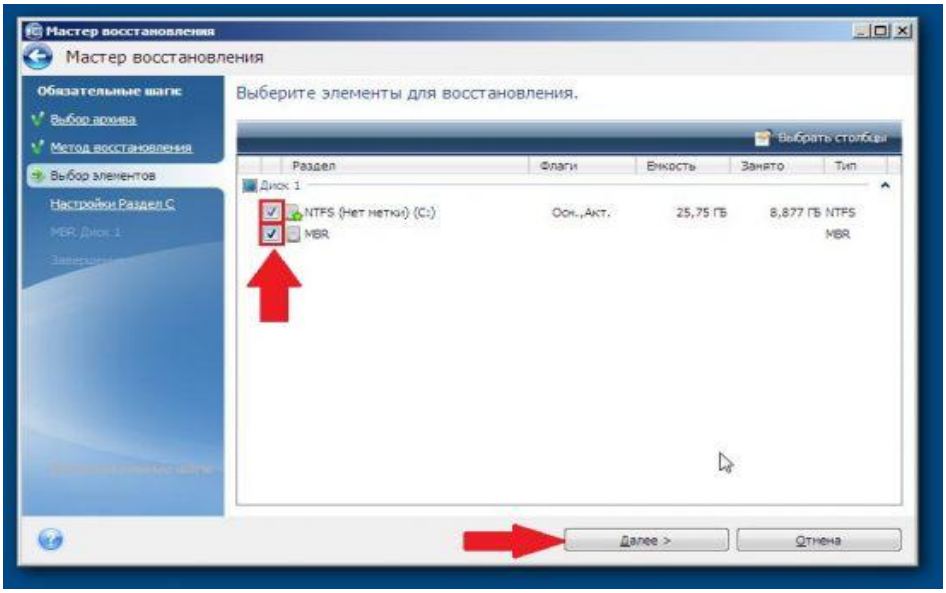
Нажав на кнопку «Обзор», выберем архив.



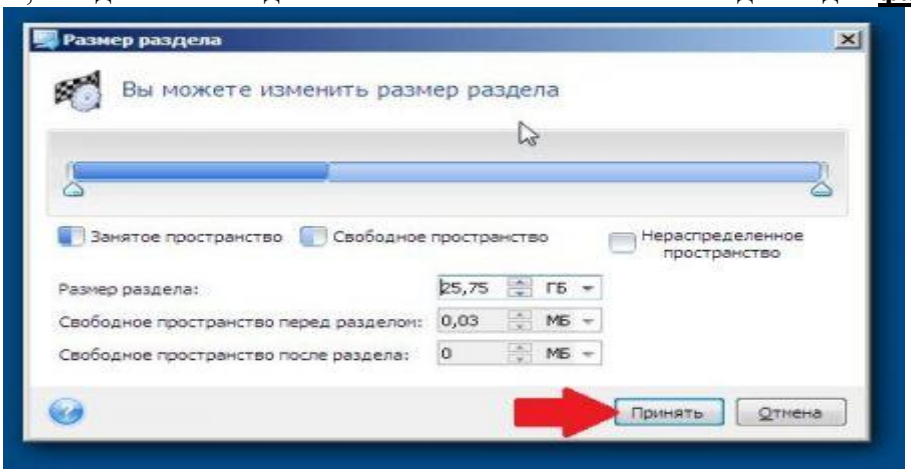
Затем, в окне «Метод восстановления», выбираем «Восстановить диски или разделы».



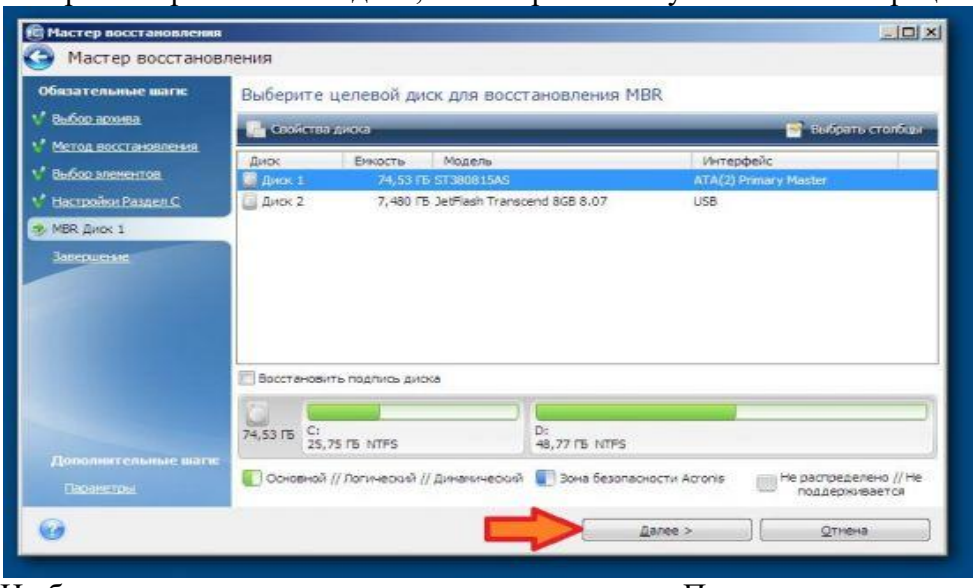
Далее ставим галку напротив восстанавливаемого диска и напротив MBR обязательно. MBR - это загрузочная область на которой прописаны файлы, которые при включении компьютера, указывают на диск с установленной системой Windows.



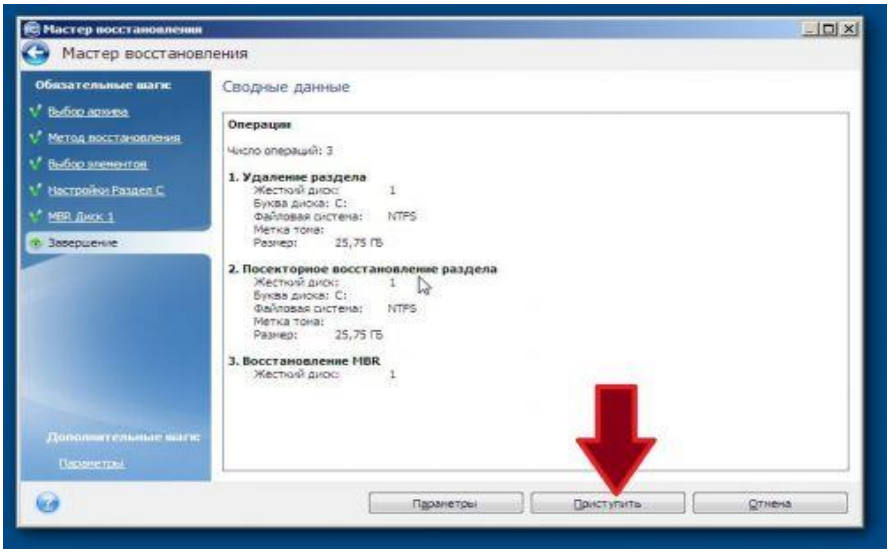
Размер раздела под систему обычно оставляют без изменений, но если позволяет место, то можно увеличить. Если много свободного места на диске С вам не к чему, можете уменьшить, но не забывайте, что должно всегда оставаться место на системном диске для **файла подкачки**.



Теперь выберем жесткий диск, на котором была установлена операционная система.



И убедившись, что все правильно, жмем кнопку «Приступить».



Восстановление раздела диска с Windows и вашими повседневными программами не займет у вас много времени, зато вы снова будете наслаждаться девственной, не замусоренной системой. В зависимости от версии AcronisTrueImage, некоторые элементы в программе могут различаться, но лишь незначительно. Время не стоит на месте и программы, да и сама винда постоянно обновляются, поэтому поневоле приходится заново устанавливать операционную систему и обновленные программы. Но если вы не гонитесь за прогрессом и вас устраивают ваши старые версии программ, то вы очень долго можете восстанавливать свою систему этим способом.

ЛАБОРАТОРНАЯ РАБОТА 6
ТЕМА: Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ
ЦЕЛЬ: ИЗУЧЕНИЕ ШИФРОВАНИЯ ИНФОРМАЦИИ МЕТОДОМ ПЕРЕСТАНОВКИ и МЕТОДОМ ЗАМЕНЫ

ШИФРЫ ПЕРЕСТАНОВКИ.

Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста.

ШИФР ПЕРЕСТАНОВКИ "СКИТАЛА". Известно, что в V веке до нашей эры правители Спарты, наиболее воинственного из греческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью ***скитала,***первого простейшего криптографического устройства, реализующего метод простой перестановки.

Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который назывался скитала, наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения. Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично.

Рисунок. Шифр "Скитала"

Такой же результат можно получить, если буквы сообщения писать по кольцу не подряд, а через определенное число позиций до тех пор, пока не будет исчерпан весь текст. Сообщение "**НАСТУПАЙТЕ**" при размещении его по окружности стержня по три буквы дает шифртекст: "**НУТАПЕСА_ТЙ**".

Для расшифрования такого шифртекста нужно не только знать правило шифрования, но и обладать ключом в виде стержня определенного диаметра. Зная только вид шифра, но не имея ключа, расшифровать сообщение было непросто.

ШИФРУЮЩИЕ ТАБЛИЦЫ. С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. В разработанных шифрах перестановки того времени применяются шифрующие таблицы, которые, в сущности, задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются: размер таблицы; слово или фраза, задающие перестановку; особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром скитала. Например, сообщение "**ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ**"записывается в таблицу поочередно по столбцам. Результат заполнения таблицы из 5 строк и 7 столбцов показан на рисунке.

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам. Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение: "**ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ**".

Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

Рисунок. Заполнение шифрующей таблицы из 5 строк и 7 столбцов

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровании действия выполняют в обратном порядке.

ШИФРЫ ЗАМЕНЫ.

Шифрами замены называются такие шифры, преобразования из которых приводят к замене каждого символа открытого текста на другие символы – шифрообозначения, причем порядок следования шифрообозначений совпадает с порядком следования соответствующих им символов открытого сообщения.

В ***шифре простой замены*** каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. **В *шифрах сложной замены*** для шифрования каждого символа открытого текста применяют свой шифр простой замены. Для реализации шифров сложной замены последовательно и циклически меняют используемые таблицы подстановки.

ПОЛИБИАНСКИЙ КВАДРАТ. Одним из первых шифров простой замены считается так называемый ***полибианский квадрат***. За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5x5, заполненную буквами греческого алфавита в случайном порядке .

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	×
χ	ν		φ	ι

Рисунок. Полибианский квадрат

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывалась в нижней строке таблицы, то для шифртекста брали самую верхнюю букву из того же столбца. Например, для слова "ταυροσ" получается шифртекст "Χφδμτξ".

СИСТЕМА ШИФРОВАНИЯ ЦЕЗАРЯ. Шифр Цезаря является частным случаем шифра простой замены. Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на*K* букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении*K* = 3. Такой шифр замены можно задать таблицей подстановки, содержащей соответствующие пары букв открытого текста и шифртекста. Совокупность возможных подстановок для*K*=3 показана в таблице.

Таблица подстановки шифра Цезаря

A→D	J→M	S→V
B→E	K→N	T→W
C→F	L→O	U→X
D→G	M→P	V→Y
E→H	N→Q	W→Z
F→I	O→R	X→A
G→J	P→S	Y→B
H→K	Q→T	Z→C
I→L	R→U	

ЛАБОРАТОРНАЯ РАБОТА №7

ТЕМА: Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем.

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

Использование электронной подписи позволяет осуществить:

- Контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.
- Защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.
- Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он известен только владельцу, он не может отказаться от своей подписи под документом.
- Доказательное подтверждение авторства документа: Так как создать корректную подпись можно, лишь зная закрытый ключ, а он известен только владельцу, он может доказать своё авторство подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

Существует несколько схем построения цифровой подписи:

- На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.
- На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем. Их появление обусловлено разнообразием задач, решаемых с помощью ЭП.

Симметричная схема

Симметричные схемы ЭП менее распространены чем асимметричные, так как после появления концепции цифровой подписи не удалось реализовать эффективные алгоритмы подписи, основанные на известных в то время симметричных шифрах.Первыми, кто обратил внимание на возможность симметричной схемы цифровой подписи, были основоположники самого понятия ЭП Диффи и Хеллман, которые опубликовали описание алгоритма подписи одного бита с помощью блочного шифра. Асимметричные схемы цифровой подписи опираются на вычислительно сложные задачи, сложность которых ещё не доказана, поэтому невозможно определить, будут ли эти схемы сломаны в ближайшее время, как это произошло со схемой, основанной назадаче об укладке ранца. Также для увеличения криптостойкости нужно увеличивать длину ключей, что приводит к необходимости переписывать программы, реализующие асимметричные схемы, и в некоторых случаях перепроектировать аппаратуру. Симметричные схемы основаны на хорошо изученных блочных шифрах.

В связи с этим симметричные схемы имеют следующие преимущества:

- Стойкость симметричных схем ЭП вытекает из стойкости используемых блочных шифров, надежность которых также хорошо изучена.
- Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

Однако у симметричных ЭП есть и ряд недостатков:

- Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.
- Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписывания раскрывается половина секретного ключа.

Из-за рассмотренных недостатков симметричная схема ЭЦП Диффи-Хелмана не применяется, а используется её модификация, разработанная Березиным и Дорошкевичем, в которой подписывается сразу группа из нескольких бит. Это приводит к уменьшению размеров подписи, но к увеличению объёма вычислений. Для преодоления проблемы «одноразовости» ключей используется генерация отдельных ключей из главного ключа.

Асимметричная схема

Асимметричные схемы ЭП относятся к криптосистемам с открытым ключом. В отличие от асимметричных алгоритмов шифрования, в которых шифрование производится с помощью открытого ключа, а расшифровка — с помощью закрытого, в схемах цифровой подписи подписание производится с применением закрытого ключа, а проверка подписи — с применением открытого.

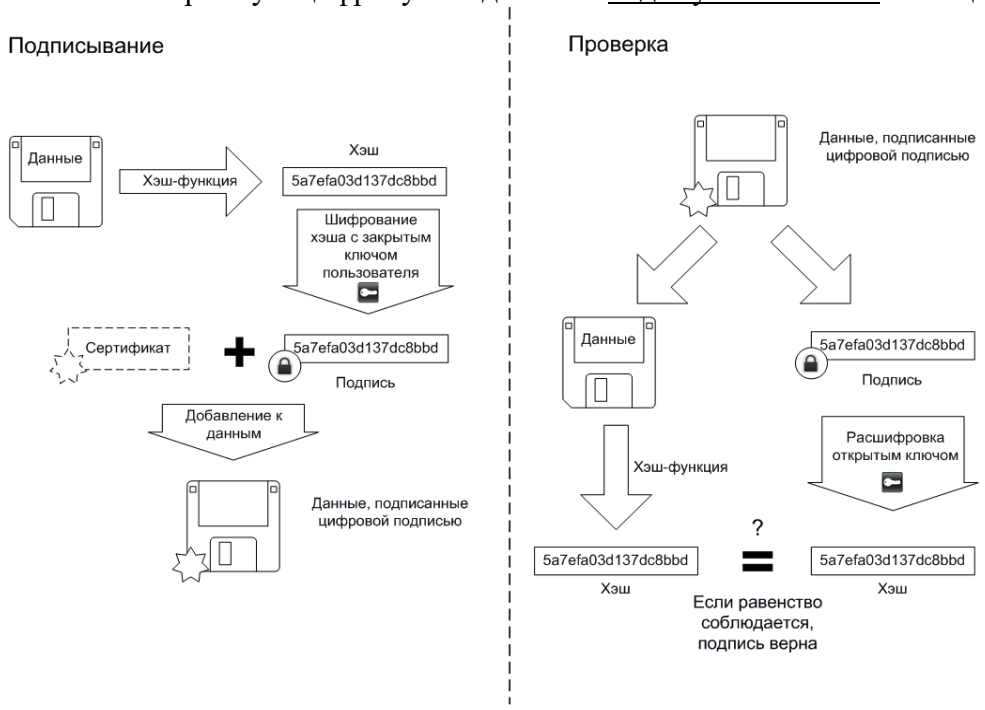
Общепризнанная схема цифровой подписи охватывает три процесса:

- Генерация ключевой пары. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.
- Формирование подписи. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись.
- Проверка (верификация) подписи. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи.

Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:

- Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.
- Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.

Следует отличать электронную цифровую подпись от кода аутентичности сообщения (MAC).



Подделка документа (коллизия первого рода)

Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в следующем:

- Документ представляет из себя осмысленный текст.
- Текст документа оформлен по установленной форме.
- Документы редко оформляют в виде PlainText-файла, чаще всего в формате DOC или HTML.

Если у фальшивого набора байт и произойдет коллизия с хэшем исходного документа, то должны выполниться 3 следующих условия:

- Случайный набор байт должен подойти под сложно структурированный формат файла.
- То, что текстовый редактор прочитает в случайном наборе байт, должно образовывать текст, оформленный по установленной форме.
- Текст должен быть осмысленным, грамотным и соответствующим теме документа.

Впрочем, во многих структурированных наборах данных можно вставить произвольные данные в некоторые служебные поля, не изменив вид документа для пользователя. Именно этим пользуются злоумышленники, подделывая документы. Некоторые форматы подписи даже защищают целостность текста, но не служебных полей.

Вероятность подобного происшествия также ничтожно мала. Можно считать, что на практике такого случиться не может даже с ненадёжными хэш-функциями, так как документы обычно большого объёма — килобайты.

Получение двух документов с одинаковой подписью (коллизия второго рода)

Куда более вероятна атака второго рода. В этом случае злоумышленник фабрикует два документа с одинаковой подписью, и в нужный момент подменяет один другим. При использовании надёжной хэш-функции такая атака должна быть также вычислительно сложной. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хэширования MD5.

Социальные атаки

Социальные атаки направлены не на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами.Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа.Злоумышленник может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи.Злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.

Использование протоколов обмена ключами и защита закрытого ключа от несанкционированного доступа позволяет снизить опасность социальных атак.

Управление открытыми ключами. Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭП, является управление открытыми ключами. Так как открытый ключ доступен любому пользователю, то необходим механизм проверки того, что этот ключ принадлежит именно своему владельцу. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя, защитить эти ключи от подмены злоумышленником, а также организовать отзы́в ключа в случае его компрометации.

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица. Существуют системы сертификатов двух типов: централизованные и децентрализованные. В децентрализованных системах путём перекрёстного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия. В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями.

Центр сертификации формирует закрытый ключ и собственный сертификат, формирует сертификаты конечных пользователей и удостоверяет их аутентичность своей цифровой подписью. Также центр проводит отзы́в истекших и компрометированных сертификатов и ведёт базы(списки) выданных и отозванных сертификатов. Обратившись в сертификационный центр, можно получить собственный сертификат открытого ключа, сертификат другого пользователя и узнать, какие ключи отозваны.

Хранение закрытого ключа

Смарт-карта и USB-брелоки

Закрытый ключ является наиболее уязвимым компонентом всей криптосистемы цифровой подписи. Злоумышленник, укравший закрытый ключ пользователя, может создать действительную цифровую подпись любого электронного документа от лица этого пользователя. Поэтому особое внимание нужно уделять способу хранения закрытого ключа. Пользователь может хранить закрытый ключ на своем персональном компьютере, защитив его с помощью пароля. Однако такой способ хранения имеет ряд недостатков, в частности, защищённость ключа полностью зависит от защищённости компьютера, и пользователь может подписывать документы только на этом компьютере.

ЛАБОРАТОРНАЯ РАБОТА №8

ТЕМА: Изучение принципов идентификации и механизмов подтверждения подлинности пользователя. Правила формирования электронной цифровой подписи

Прежде чем получить доступ к КС, пользователь должен идентифицировать себя, а затем средства защиты сети должны подтвердить подлинность этого пользователя, т.е. проверить, является ли данный пользователь действительно тем, за кого он себя выдает. Компоненты механизма защиты легальных пользователей размещены на рабочей ЭВМ, к которой подключен пользователь через его терминал (или каким-либо иным способом). Поэтому процедуры идентификации, подтверждения подлинности и наделения полномочиями выполняются в начале сеанса на местной рабочей ЭВМ.

Когда пользователь начинает работу в КС, используя терминал, система запрашивает его имя и идентификационный номер. В зависимости от ответов пользователя компьютерная система проводит его идентификацию. Затем система проверяет, является ли пользователь действительно тем, за кого он себя выдает. Для этого она запрашивает у пользователя пароль. Пароль - это лишь один из способов подтверждения подлинности пользователя.

Перечислим возможные способы подтверждения подлинности.

- Предопределенная информация, находящаяся в распоряжении пользователя: пароль, персональный идентификационный номер, соглашение об использовании специальных закодированных фраз.
- Элементы аппаратного обеспечения, находящиеся в распоряжении пользователя: ключи, магнитные карточки, микросхемы и т.п.
- Характерные личные особенности пользователя: отпечатки пальцев, рисунок сетчатки глаза, тембр голоса и т.п.
- Характерные приемы и черты поведения пользователя в режиме реального времени: особенности динамики и стиль работы на клавиатуре, приемы работы с манипулятором и т.п.
- Навыки и знания пользователя, обусловленные образованием, культурой, обучением, воспитанием, привычками и т.п.

Применение пароля для подтверждения подлинности пользователя. Традиционно каждый законный пользователь компьютерной системы получает идентификационный номер и/или пароль. В начале сеанса работы на терминале пользователь указывает свой идентификационный номер (идентификатор пользователя) системе, которая затем запрашивает у пользователя пароль.

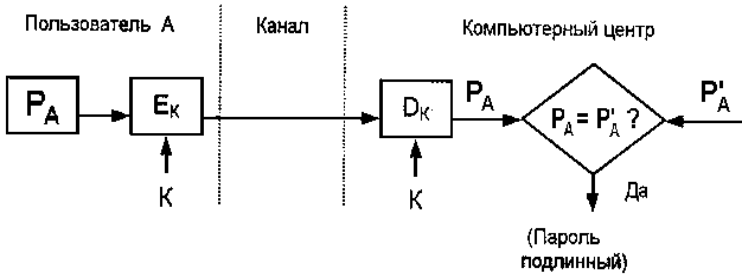


Рис.1. Схема простой аутентификации с помощью пароля

Простейший метод подтверждения подлинности с использованием пароля основан на сравнении представляемого пользователем пароля P_A с исходным значением P'_A, хранящимся в компьютерном центре (рис.1). Поскольку пароль должен храниться в тайне, его следует шифровать перед пересылкой по незащищенному каналу. Если значения P_A и P'_A совпадают, то пароль P_A считается подлинным, а пользователь - законным. Если кто-нибудь, не имеющий полномочий для входа в систему, узнает каким-либо образом пароль и идентификационный номер законного пользователя, он получит доступ в систему.

Иногда получатель не должен раскрывать исходную открытую форму пароля. В этом случае отправитель должен пересылать вместо открытой формы пароля отображение пароля, получаемое с использованием односторонней функции $\square(\cdot)$ пароля. Это преобразование должно гарантировать невозможность раскрытия противником пароля по его отображению, так как противник наталкивается на неразрешимую числовую задачу.

Например, функция □ (·) может быть определена следующим образом:□(P) = E_P(ID),где P - пароль отправителя; ID - идентификатор отправителя;E_P - процедура шифрования, выполняемая с использованием пароля P в качестве ключа.

Такие функции особенно удобны, если длина пароля и длина ключа одинаковы. В этом случае подтверждение подлинности с помощью пароля состоит из пересылки получателю отображения □(P) и сравнения его с предварительно вычисленным и хранимым эквивалентом □'(P).

На практике пароли состоят только из нескольких букв, чтобы дать возможность пользователям запомнить их. Короткие пароли уязвимы к атаке полного перебора всех вариантов. Для того чтобы предотвратить такую атаку, функцию □(P) определяют иначе,а именно:

□ (P)=$E_{P□K}$(ID),

где K и ID - соответственно ключ и идентификатор отправителя.

Очевидно, значение □ (P) вычисляется заранее и хранится в виде □'(P) в идентификационной таблице у получателя (рис. 2). Подтверждение подлинности состоит из сравнения двух отображений пароля □(P_A) и □(P_A) и признания пароля P_A, если эти отображения равны. Конечно, любой, кто получит доступ к идентификационной таблице, может незаконно изменить ее содержимое, не опасаясь, что эти действия будут обнаружены.

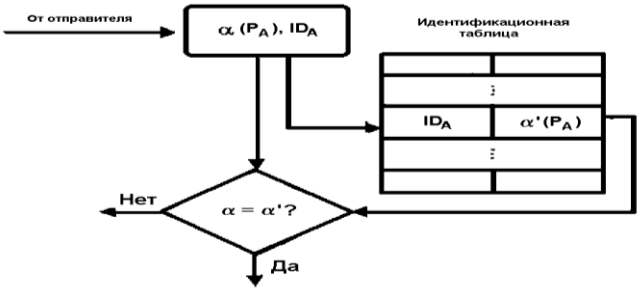


Рис. 2. Схема аутентификации с помощью пароля с использованием идентификационной таблицы

Взаимная проверка подлинности пользователей

Обычно стороны, вступающие в информационный обмен, нуждаются во взаимной проверке подлинности (аутентификации) друг друга. Этот процесс взаимной аутентификации выполняют в начале сеанса связи.

Для проверки подлинности применяют следующие способы:

- механизм запроса-ответа;
- механизм отметки времени ("временной штемпель").

Механизм запроса-ответа состоит в следующем. Если пользователь. А хочет быть уверенным, что сообщения, получаемые им от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент - запрос X (например, некоторое случайное число). При ответе пользователь В должен выполнить над этим элементом некоторую операцию (например, вычислить некоторую функцию f(X)). Это невозможно осуществить заранее, так как пользователю В неизвестно, какое случайное число X придет в запросе. Получив ответ с результатом действий В, пользователь А может быть уверен, что В - подлинный. Недостаток этого метода - возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить, насколько "устарело" пришедшее сообщение, и решить не принимать его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает проблема допустимого временного интервала задержки для подтверждения подлинности сеанса. Ведь сообщение с "временным штемпелем" в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы. Какое запаздывание "штемпеля" является подозрительным?

Для взаимной проверки подлинности обычно используют процедуру рукопожатия. Эта процедура базируется на указанных выше механизмах контроля и заключается во взаимной

проверке ключей, используемых сторонами. Иначе говоря, стороны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами. Процедуру рукопожатия обычно применяют в компьютерных сетях при организации сеанса связи между пользователями, пользователем и хост-компьютером, между хост-компьютерами и т.д. Рассмотрим в качестве примера процедуру рукопожатия для двух пользователей А и В. (Это допущение не влияет на общность рассмотрения. Такая же процедура используется, когда вступающие в связь стороны не являются пользователями). Пусть применяется симметричная криптосистема. Пользователи А и В разделяют один и тот же секретный ключ K_{AB}. Вся процедура показана на рисунке.

- Пусть пользователь А инициирует процедуру рукопожатия, отправляя пользователю В свой идентификатор ID_A в открытой форме.
- Пользователь В, получив идентификатор ID_A, находит в базе данных секретный ключ K_{AB} и вводит его в свою криптосистему.

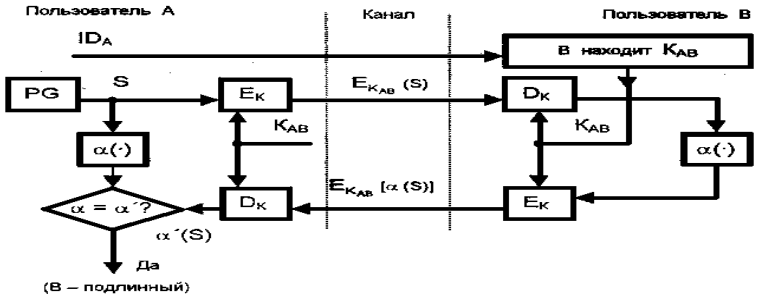


Рис.3.Схема процедуры рукопожатия (пользователь А проверяет подлинность пользователя В)

- Тем временем *пользователь А* генерирует случайную последовательность S с помощью псевдослучайного генератора PG и отправляет ее *пользователю В* в виде криптограммы$E_{K\square B}$(S).
- Пользователь В расшифровывает эту криптограмму и раскрывает исходный вид последовательности S.
- Затем оба пользователя А и В преобразуют последовательность S, используя открытую одностороннюю функцию □(·).
- Пользователь В шифрует сообщение □ S) и отправляет эту криптограмму *пользователю А.*
- Наконец, пользователь А расшифровывает эту криптограмму и сравнивает полученное сообщение □'(S) с исходным □(S). Если эти сообщения равны, пользователь А признает подлинность пользователя В.

Очевидно, пользователь В проверяет подлинность пользователя А таким же способом. Обе эти процедуры образуют процедуру рукопожатия, которая обычно выполняется в самом начале любого сеанса связи между любыми двумя сторонами в компьютерных сетях.

Достоинством модели рукопожатия является то, что ни один из участников сеанса связи не получает никакой секретной информации во время процедуры подтверждения подлинности.

Иногда пользователи хотят иметь непрерывную проверку подлинности отправителей в течение всего сеанса связи. Один из простейших способов непрерывной проверки подлинности показан на рис. 4. Передаваемая криптограмма имеет видE_K (ID_A, M),где ID_A - идентификатор отправителя А; M - сообщение.

Получатель В, принявший эту криптограмму, расшифровывает ее и раскрывает пару (ID_A, M). Если принятый идентификатор ID_A совпадает с хранимым значением ID_A'(получатель В признает эту криптограмму.

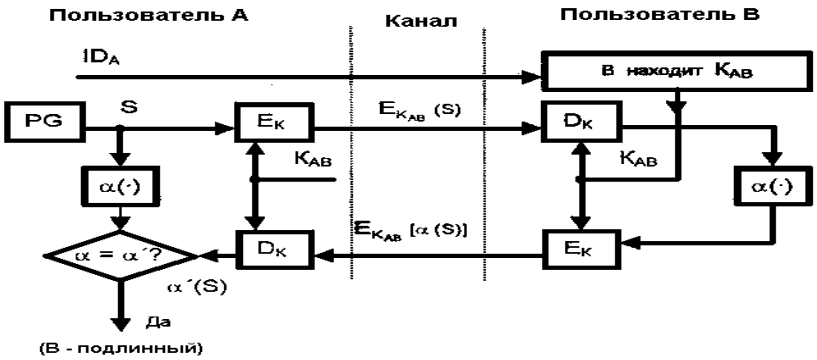


Рис. 4. Схема непрерывной проверки подлинности отправителя

Другой вариант непрерывной проверки подлинности использует вместо идентификатора отправителя его секретный пароль. Заранее подготовленные пароли известны обеим сторонам. Пусть P_A и P_B - пароли пользователей А и В соответственно. Тогда пользователь А создает криптограмму

$C = E_K (P_A, M)$.

Получатель криптограммы расшифровывает ее и сравнивает пароль, извлеченный из этой криптограммы, с исходным значением. Если они равны, получатель признает эту криптограмму.

Процедура рукопожатия была рассмотрена в предположении, что пользователи А и В уже имеют общий *секретный сеансовый ключ.* Реальные процедуры предназначены для распределения ключей между подлинными партнерами и включает как этап распределения ключей, так и этап собственно подтверждения подлинности партнеров по информационному обмену.

ЛАБОРАТОРНАЯ РАБОТА№9

ТЕМА: Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.

Реализация информационных технологий защиты продуктом сетевой безопасности CHECK POINT FIREWALL-1

CheckPointSoftwareTechnologies предлагает комплексное решение, соответствующее новым и постоянно возрастающим требованиям по обеспечению безопасности ИВС предприятия. Пример организации ИВС предприятия с применением межсетевых экранов показан на рисунке 1..

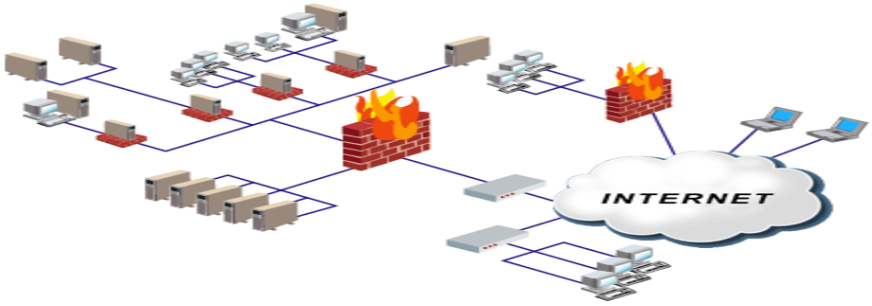


Рисунок 1. Пример организации ИВС с применением межсетевых экранов

Комплект продуктов сетевой безопасности, называемый CheckPoint FireWall-1, обеспечивает контроль доступа в сетях Интернет, Интранет, Экстранет, а также удалённого доступа с расширенными функциями авторизации и установления подлинности пользователей. FireWall-1 позволяет транслировать сетевые адреса (NAT) и сканировать потоки данных на наличие недопустимой информации и вирусов. Широкий набор основных и сервисных функций даёт возможность реализовать интегрированное решение по обеспечению сетевой и информационной безопасности, полностью отвечающее современным требованиям любых организаций.

Возможности межсетевой экран CheckPoint Firewall-1:

- защита корпоративных ресурсов от внешних и внутренних злоумышленников;
- аутентификация внешних и внутренних пользователей для доступа к защищаемым ресурсам корпоративной сети и ресурсам Internet;
- поддержка более 150 сетевых сервисов, протоколов и приложений (включая, H.323, VoIP, RealAudio, Oracle SQL и т.д.);
- скрытие сетевой топологии защищаемой сети;
- защита от вирусов, враждебного мобильного кода (Java, ActiveX, ShockWave и т.д.), а также фильтрация содержания Internet-трафика;
- централизованное управление безопасностью удалённых офисов и филиалов;
- поддержка большого числа платформ;
- различные уровни доступа по управлению межсетевым экраном;
- обеспечение высокой доступности и отказоустойчивости;
- управление списками контроля доступа маршрутизаторов и серверов удалённого доступа;
- балансировка нагрузки между несколькими узлами;
- генерация большого числа различных отчётов, имеющих как графическое, так и текстовое представление.

FireWall-1 позволяет предприятию создать единую интегрированную политику безопасности, которая распространялась бы на множество межсетевых экранов и управлялась бы с любой выбранной для этого точки сети предприятия. Продукт имеет и дополнительные возможности:

- управление списками доступа аппаратных маршрутизаторов,
- балансировка сетевой нагрузки на серверы,
- элементы для построения систем повышенной надёжности, которые также полностью интегрируются в глобальную политику безопасности.

Работа CheckPoint FireWall-1 прозрачна для пользователей и обеспечивает рекордную производительность практически для любого IP протокола и высокоскоростной технологии передачи данных.

Компоненты межсетевого экрана FIREWALL-1

Межсетевой экран CheckPoint Firewall-1 использует трёхуровневую архитектуру и состоит из следующих компонентов (рисунок 2).FirewallModule, который реализует все функции по разграничению доступа, регистрации событий, генерации сигналов тревоги и т.д.

ManagementServer, который управляет всеми подключёнными к нему модулями. При этом ManagementServer может управлять не только FirewallModule, но и другими компонентами, входящими в семейство решений компании CheckPoint (например, VPN Module, FloodGateModule и т.д.).Консоль управления (GUI), которая реализует графический интерфейс, облегчающий управление всеми модулями, подключёнными к ManagementServer.

Рисунок 2 Трёхуровневая архитектура межсетевого экрана CheckPoint Firewall-1

В зависимости от технологии обработки информации, принятой в организации, может использоваться две схемы применения межсетевого экрана CheckPoint Firewall-1 & VPN-1:локальная,распределённая.

Первая схема предназначена для тех случаев, когда организация (как правило, небольшого размера) имеет только одну точку выхода в сети открытого доступа, которая и защищается при помощи межсетевого экрана. В этом случае целесообразно применять FirewallInternetGateway (или VPN-1 InternetGateway), который включает в себя Firewall (или VPN) Module и ManagementServer, и устанавливается на выделенном компьютере. Консоль управления (GUI) при этом устанавливается в удобном для администратора месте. В данном случае ManagementServer управляет только одним Firewall (или VPN) Module.

Вторая схема используется в крупных, территориально-распределённых организациях, и предполагает распределённую установку Firewall (или VPN) Module и ManagementServer. Модули, отвечающие за разграничение доступа к корпоративным ресурсам и построение VPN, устанавливаются в заранее определённых местах, и управляются с одного сервера управления. Как и в предыдущем случае, консоль (или несколько консолей) управления может быть установлена в любом месте. Данный вариант описывается схемой n * Firewall (VPN) Module + EnterpriseConsole (где n – число мест установки компонентов, входящих в семейство решений CheckPoint).

Основываясь на технологии инспекции пакетов с учетом состояния протокола, являющейся передовым методом контроля сетевого трафика, разработанного и запатентованного компанией CheckPoint, FireWall-1 обеспечивает наивысший уровень безопасности. Данный метод обеспечивает сбор информации из пакетов данных, как коммуникационного, так и прикладного уровня, что достигается сохранением и накоплением ее в специальных контекстных таблицах, которые динамически обновляются. Такой подход обеспечивает полный контроль даже за уровнем приложения без необходимости введения отдельного приложения-посредника (proxy) для каждого защищаемого сетевого сервиса.

Трансляция сетевых адресов (NAT) используется для организации доступа корпоративных пользователей к узлам общей сети с компьютеров защищаемой сети. Характеристики IP-пакетов, для которых используется трансляция адресов, определяются с помощью правил трансляции. Существуют два типа правил трансляции:исходящие;входящие.

Исходящие правила трансляции применяются тогда, когда инициатором соединения является абонент защищенной сети. В этом случае в исходящих IP-пакетах, истинный IP-адрес отправителя заменяется на указанный в правиле трансляции мнимый IP-адрес, а входящие IP-пакеты перенаправляются отправителю на его истинный IP-адрес.

Входящие правила трансляции применяются тогда, когда инициатором соединения является сторонний абонент, например, пользователь глобальной сети, которому известен только мнимый IP-адрес получателя, заданный исходящим правилом трансляции. В этом случае входящие IP-пакеты перенаправляются получателю на его истинный IP-адрес, а исходящие IP-пакеты содержат его мнимый IP-адрес.

ЛАБОРАТОРНАЯ РАБОТА №10
ТЕМА: Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия.
ЦЕЛЬ: ИЗУЧИТЬ СИСТЕМЫ ОБНАРУЖЕНИЕ АТАК

Системы обнаружения компьютерных атак (IDS - IntrusionDetectionSystems) - один из важнейших элементов систем информационной безопасности сетей любого современного предприятия, учитывая, как растет в последние годы число проблем, связанных с компьютерной безопасностью. Хотя технология IDS не обеспечивает полную защиту информации, тем не менее она играет весьма заметную роль в этой области.

Цель любой IDS - обнаружить атаку с наименьшими ошибками. При этом объект атаки (жертва) обычно хочет получить ответ на следующие вопросы.

- Что случилось с моей системой?
- Что подверглось нападению, и насколько опасна атака?
- Кто злоумышленник?
- Когда атака началась и откуда?
- Как и почему произошло вторжение?

Злоумышленник, в свою очередь, как правило, пытается узнать следующее. ·

- Что представляет собой цель атаки?
- Есть ли уязвимости и какие?
- Какой вред можно нанести?
- Какие эксплойты или средства проникновения имеются?
- Есть ли риск быть раскрытым?

Классификация IDS. Для проведения классификации IDS необходимо учесть несколько факторов (рисунок 1).Метод обнаружения описывает характеристики анализатора. Когда IDS использует информацию о нормальном поведении контролируемой системы, она называется поведенческой. Когда IDS работает с информацией об атаках, она называется интеллектуальной.

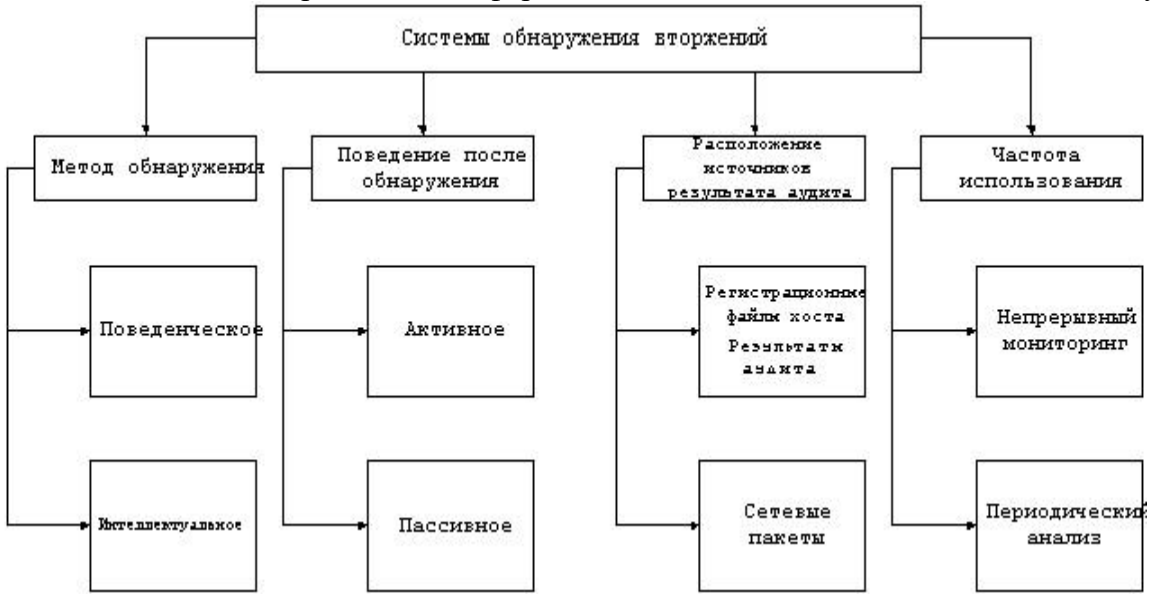


Рисунок 1. Характеристики систем обнаружения вторжений

Поведение после обнаружения указывает на реакцию IDS на атаки. Реакция может быть активной – IDS предпринимает корректирующие (устраняет лазейки) или действительно активные (закрывает доступ для возможных нарушителей, делая недоступными сервисы) действия. Если IDS только выдаёт предупреждения, её называют пассивной.

Расположение источников результата аудита подразделяет IDS в зависимости от вида исходной информации, которую они анализируют. Входными данными для них могут быть результаты аудита, системные регистрационные файлы или сетевые пакеты.

Классифицировать IDS можно также по нескольким параметрам. По **способам реагирования** различают статические и динамические IDS. Статические средства делают «снимки» (snapshot) среды и осуществляют их анализ, разыскивая уязвимое ПО, ошибки в конфигурациях и т.д. Статические IDS проверяют версии работающих в системе приложений на наличие известных уязвимостей и слабых паролей, проверяют содержимое специальных файлов в директориях пользователей или проверяют конфигурацию открытых сетевых сервисов. Статические IDS обнаруживают следы вторжения. Динамические IDS осуществляют мониторинг в реальном времени всех действий, происходящих в системе, просматривая файлы аудита или сетевые пакеты, передаваемые за определённый промежуток времени. Динамические IDS реализуют анализ в реальном времени и позволяют постоянно следить за безопасностью системы.

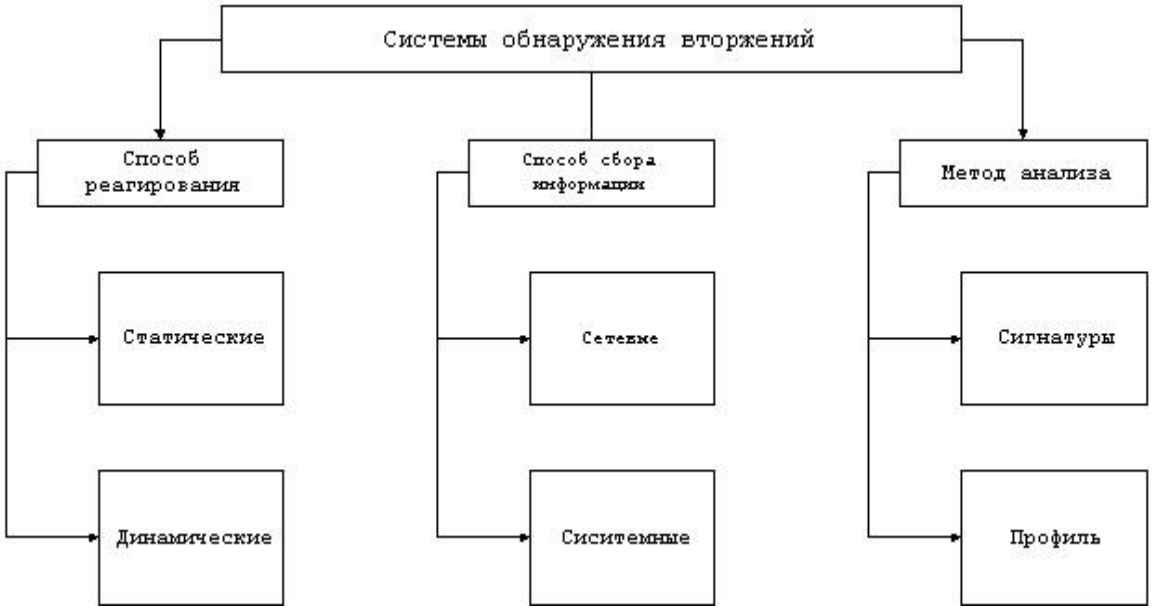


Рисунок 2. Классификация систем обнаружения вторжений

По **способу сбора информации** различают сетевые и системные IDS. Сетевые (NIDS)контролируют пакеты в сетевом окружении и обнаруживают попытки злоумышленника проникнуть внутрь защищаемой системы или реализовать атаку «отказ в обслуживании». Эти IDS работают с сетевыми потоками данных. Типичный пример NIDS – система, которая контролирует большое число TPC-запросов на соединение (SYN) со многими портами на выбранном компьютере, обнаруживая, таким образом, что кто-то пытается осуществить сканирование TCP-портов. Сетевая IDS может запускаться либо на отдельном компьютере, который контролирует свой собственный трафик, либо на выделенном компьютере, прозрачно просматривающим весь трафик в сети (концентратор, маршрутизатор). Сетевые IDS контролируют много компьютеров, тогда как другие IDS контролируют только один. IDS, которые устанавливаются на хосте и обнаруживают злонамеренные действия на нём называютсяхостовыми или системными IDS. Примерами хостовых IDS могут быть системы контроля целостности файлов (СКЦФ), которые проверяют системные файлы с целью определения, когда в них были внесены изменения. Мониторы регистрационных файлов (Log-filemonitors, LFM), контролируют регистрационные файлы, создаваемые сетевыми сервисами и службами. Обманные системы, работающие с псевдосервисами, цель которых заключается в воспроизведении хорошо известных уязвимостей для обмана злоумышленников.

По **методам анализа** IDS делят на две группы: IDS, которые сравнивают информацию с предустановленной базой сигнатур атак и IDS, контролирующие частоту событий или обнаружение статистических аномалий.

Анализ сигнатур был первым методом, примененным для обнаружения вторжений. Он базируется на простом понятии совпадения последовательности с образцом. Во входящем пакете просматривается байт за байтом и сравнивается с сигнатурой (подписью) – характерной строкой программы, указывающей на характеристику вредного трафика. Такая подпись может содержать

ключевую фразу или команду, которая связана с нападением. Если совпадение найдено, объявляется тревога.

Второй метод анализа состоит в рассмотрении строго форматированных данных трафика сети, известных как протоколы. Каждый пакет сопровождается различными протоколами. Авторы IDS, зная это, внедрили инструменты, которые разворачивают и осматривают эти протоколы, согласно стандартам. Каждый протокол имеет несколько полей с ожидаемыми или нормальными значениями. Если что-нибудь нарушает эти стандарты, то вероятна злонамеренность. IDS просматривает каждое поле всех протоколов входящих пакетов: IP, TCP, и UDP. Если имеются нарушения протокола, например, если он содержит неожиданное значение в одном из полей, объявляется тревога

Работа современных IDS и различные виды атак

Общая схема функционирования IDS приведена на рис. 3. В последнее время появилось много публикаций о системах, называемых distributed IDS (dIDS). dIDS состоит из множества IDS, которые расположены в различных участках большой сети и связаны между собой и с центральным управляющим сервером. Такая система усиливает защищенность корпоративной подсети благодаря централизации информации об атаке от различных IDS. dIDS состоит из следующих подсистем: центральный анализирующий сервер, агенты сети, сервер сбора информации об атаке.

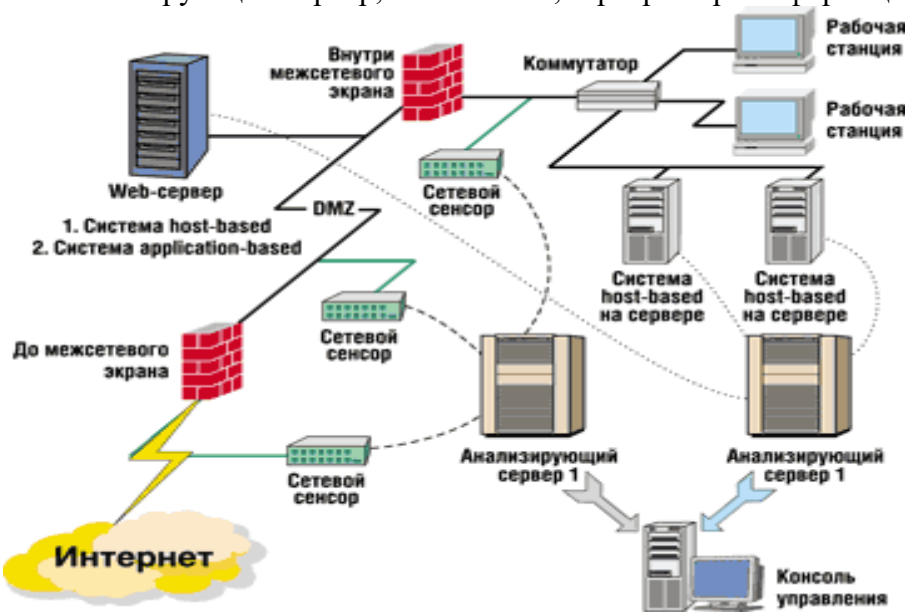


Рисунок3. Общая схема функционирования IDS.

Центральный анализирующий сервер обычно состоит из базы данных и Web-сервера, что позволяет сохранять информацию об атаках и манипулировать данными с помощью удобного Web-интерфейса. Агент сети - один из наиболее важных компонентов dIDS. Он представляет собой небольшую программу, цель которой - сообщать об атаке на центральный анализирующий сервер.

Сервер сбора информации об атаке - часть системы dIDS, логически базирующаяся на центральном анализирующем сервере. Сервер определяет параметры, по которым группируется информация, полученная от агентов сети. Группировка может осуществляться по следующим параметрам: IP-адресу атакующего; порту получателя; номеру агента; дате, времени; протоколу; типу атаки и т. д.

Несмотря на многочисленные упреки и сомнения в работоспособности IDS, пользователи уже широко применяют как коммерческие средства, так и свободно распространяемые. Разработчики оснащают свои продукты возможностями активного реагирования на атаку. Система не только определяет, но и пытается остановить атаку, а также может провести ответное нападение на атакующего. Наиболее распространенные типы активного реагирования - прерывание сессии и переконфигурирование межсетевого экрана.

При этом необходимо помнить, что уже существуют средства для выявления IDS, работающих в режиме "прослушивания" трафика; кроме того, многие IDS подвержены атакам типа DoS (отказ в обслуживании).

Компании и продукты. На рынке представлено несколько десятков коммерческих систем IDS, что обеспечивает выбор наиболее приемлемого решения. К сожалению, отечественные продукты пока отсутствуют, хотя две российские компании к концу этого года готовят выпуск своих систем обнаружения атак.Ниже описаны продукты некоторых компаний.

1. *CiscoSystems.*Серия продуктов Cisco IDS содержит решения для различных уровней. В нее входят три системы 42xx версии v.2.2.1 (network-based), среди которых 4210 (рис. 3) оптимизирована для среды 10/100Base-T (45 Мбит/с), 4235 - для среды 10/100/1000Base-TX, (200 Мбит/с) и 4250 - для 10/100/1000Base-TX (500 Мбит/с).

Подсистема IDS имеетсявкоммутатореCatalyst - Catalyst 6000 Intrusion Detection System Module (swithed-integrated network-based).

Рисунок 4 Внешний вид системы IDS 4210 CiscoSystems, установленной в стойку.

2. *InternetSecuritySystems.*Компания ISS в свое время совершила резкий скачок в данной области и занимает ведущие позиции в части реализации систем обнаружения атак. Она также предлагает целое семейство решений для различных уровней.

RealSecureNetworkSensor - программное решение, предназначенное для установки на выделенный компьютер в критичном сегменте сети. Анализируя сетевой трафик и сопоставляя его с базой сигнатур атак, сенсор обнаруживает различные нарушения политики безопасности (рис. 5).

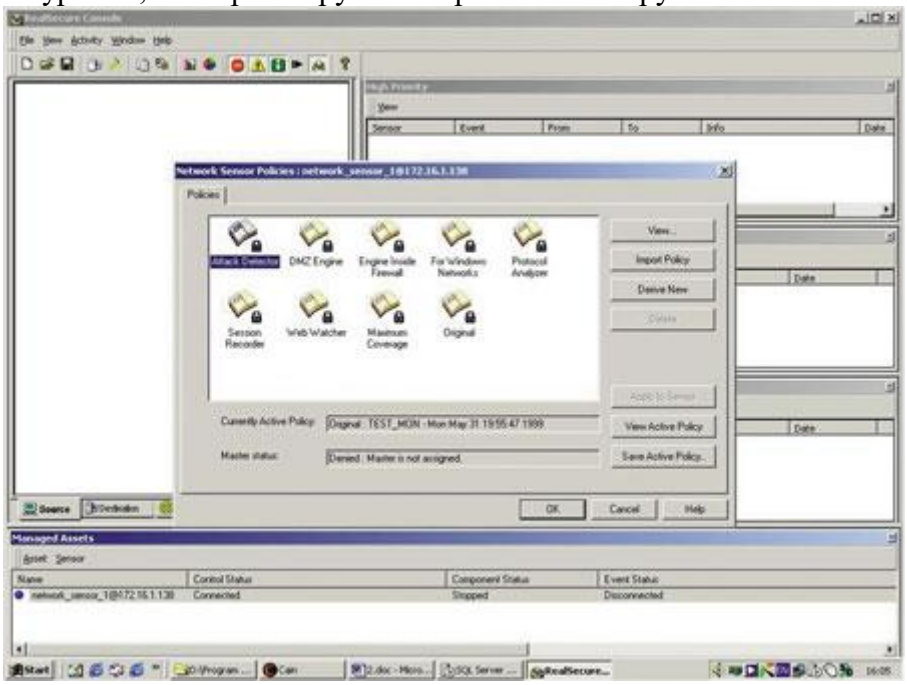


Рисунок 5. Выбор политики защиты для одного из сетевых сенсоров IDS фирмы ISS с использованием управляющей программы RealSecureConsole.

Система RealSecureGigabitSensor обрабатывает более 500 тыс. пакетов в секунду, используя запатентованный алгоритм семиуровневого анализа, обнаруживает большое число атак, пропускаемых другими системами. Применяется главным образом в сетях, работающих с большой нагрузкой.

RealSecureServerSensor позволяет обнаруживать атаки на всех уровнях, направленные на конкретный узел сети. Кроме того, может проводить анализ защищенности и обнаружения уязвимостей на контролируемом узле.

Программа RealSecureDesktopProtector (ранее называвшаяся BlackICEAgent) предназначена для обнаружения в реальном режиме времени атак, направленных на рабочие станции корпоративной сети.

RealSecureforNokia - программно-аппаратное решение, разработанное компаниями ISS и Nokia. Оно объединяет все функциональные возможности RealSecureNetworkSensor и Nokia IP NetworkSecuritySolutions. Система функционирует под управлением защищенной ОС IPSO, базирующейся на FreeBSD.

RealSecureGuard - программное решение, совмещающее в себе возможности межсетевого экрана и системы обнаружения атак в реальном режиме времени. Она устанавливается между защищаемым и открытым сегментами сети (так называемая inline-IDS) и анализирует весь проходящий через нее трафик в поисках запрещенных или опасных пакетов. Система может обнаруживать атаки как на сегменты сети, так и на отдельные, наиболее важные узлы.

Возможности системы RealSecure. Система RealSecure™ является одним из лучших решений для защиты Вашей корпоративной сети и следующих ключевых возможностей:

- большое число распознаваемых атак;
- задание шаблонов фильтрации трафика;
- централизованное управление модулями слежения;
- фильтрация и анализ большого числа сетевых протоколов, в т.ч. TCP, UDP и ICMP;
- фильтрация сетевого трафика по протоколу, портам и IP-адресам отправителя и получателя;
- различные варианты реагирования на атаки;
- аварийное завершение соединения с атакующим узлом;
- управление межсетевыми экранами и маршрутизаторами;
- задание сценариев по обработке атак;
- запись атаки для дальнейшего воспроизведения и анализа;
- поддержкасетевыхинтерфейсов Ethernet, Fast Ethernet и Token Ring;
- отсутствие требования использования специального аппаратного обеспечения;
- работасразличными Cryptographic Service Provider;
- установление защищенного соединения между компонентами системами, а также другими устройствами;
- наличие всеобъемлющей базы данных по всем обнаруживаемым атакам;
- отсутствие снижения производительности сети;
- работа с одним модулем слежения с нескольких консолей управления;
- мощная система генерация отчетов;
- использование протокола ODBC;
- различные форматы отчетов;
- мощная система подсказки;
- простота использования и интуитивно понятный графический интерфейс;
- невысокие системные требования к программному и аппаратному обеспечению.

Система RealSecure™ позволяет обнаруживать большое число атак и иных контролируемых событий. В версии 2.5 это число превышает 665. Ниже описаны основные типы контролируемых событий:

"Отказ в обслуживании" (Denialofservice)

Любое действие или последовательность действий, которая приводит любую часть атакуемой системы к выходу из строя, при котором та перестают выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т.д. Примером могут служить атаки SYN Flood, PingFlood, WindowsOut-of-Band (WinNuke) и т.п.

"Неавторизованный доступ" (Unauthorizedaccessattempt)

Любое действие или последовательность действий, которая приводит к попытке чтения файлов или выполнения команд в обход установленной политики безопасности. Также включает попытки злоумышленника получить привилегии, большие, чем установлены администратором системы. Примером могут служить атаки FTP Root, E-mail WIZ и т.п.

"Предварительные действия перед атакой" (Pre-attackprobe)

Любое действие или последовательность действий по получению информации ИЗ или О сети (например, имена и пароли пользователей), используемые в дальнейшем для осуществления неавторизованного доступа. Примером может служить сканирование портов (Portscan), сканирование при помощи программы SATAN (SATAN scan) и т.п.

"Подозрительная активность" (Suspiciousactivity)

Сетевой трафик, выходящий за рамки определения "стандартного" трафика. Может указывать на подозрительные действия, осуществляемые в сети. Примером могут служить события Duplicate IP Address, IP UnknownProtocol и т.п.

"Анализ протокола" (Protocoldecode)

Сетевая активность, которая может быть использована для осуществления одной из атак вышеназванных типов. Может указывать на подозрительные действия, осуществляемые в сети. Примером могут служить события FTP Userdecode, PortmapperProxydecode и т.п.

ЛАБОРАТОРНАЯ РАБОТА№11

ТЕМА: Реализация информационных технологий для построения защищенной информационно-вычислительной сети

Глобальная сеть Internet создавалась как открытая система, предназначенная для свободного обмена информацией. В силу открытости своей идеологии Internet представляет для злоумышленников значительно большие возможности по сравнению с традиционными информационными системами. Через Internet нарушитель может:

• вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации;

• незаконно скопировать важную и ценную для предприятия информацию;

• получить пароли, адреса серверов и их содержимое;

• входить в информационную систему предприятия под именем зарегистрированного пользователя .

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны. ***Межсетевой экран (МЭ)***– это система межсетевой защиты, позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя ее можно провести и внутри корпоративной сети предприятия. МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение – пропускать его или отбросить. Для того чтобы МЭ мог осуществить это, ему необходимо определить набор правил фильтрации.

Наилучшим из известных в настоящее время сертифицированных аппаратно-программных комплексов, способных решить проблему защиты от всевозможных атак "извне", является разработанный "Информзащитой" "Континент-К", являющийся реализацией идеологии VPN
(VirtualPrivateNetwork). Технология VPN позволяет формировать виртуальные защищенные каналы в сетях общего пользования (например, Internet), гарантирующие конфиденциальность и достоверность информации. VPN-сеть представляет собой объединение локальных сетей (ЛВС) или отдельных компьютеров, подключенных к сети общего пользования, в единую защищенную виртуальную сеть.

Аппаратно-программный комплекс “Континент-К” обеспечивает:

• защиту внутренних сегментов сети от несанкционированного доступа со стороны пользователей сетей общего пользования;

• скрытие внутренней структуры защищаемых сегментов сети;

• криптографическую защиту данных, передаваемых по каналам связи сетей общего пользования между защищаемыми сегментами сети (абонентскими пунктами);

• безопасный доступ пользователей VPN к ресурсам сетей общего пользования.

Комплекс “Континент-К” включает в свой состав следующие компоненты:

• центр управления сетью криптографических шлюзов;

• криптографический шлюз;

• программа управления сетью криптографических шлюзов.

Центр управления сетью (ЦУС) осуществляет управление работой всех КШ, входящих в состав виртуальной сети. ЦУС осуществляет контроль над состоянием всех зарегистрированных КШ, проводит рассылку ключевой информации, предоставляет администратору функции удаленного управления КШ, обеспечивает получение и хранение содержимого системных журналов КШ, а также ведение журнала событий НСД.

Криптографический шлюз (КШ) обеспечивает криптографическую защиту информации при ее передаче по открытым каналам сетей общего пользования и защиту внутренних сегментов сети от проникновения извне. Программа управления обеспечивает отображение состояний КШ,

просмотр содержимого системных журналов КШ, изменение настроек маршрутизации и правил фильтрации пакетов.

Комплекс *“Континент-К”* может использоваться в следующих вариантах: • защита соединения «точка-точка»; • защищенная корпоративная VPN-сеть.

Защита соединения «точка-точка» (рис. 1) предполагает использование КШ для защиты данных, передаваемых по неконтролируемой территории между двумя защищенными сегментами территориально разделенных ЛВС через сеть Internet или по выделенному каналу связи.

Рис. 1. Защита соединения «точка-точка»

В этом случае обеспечивается шифрование и имитозащита данных, передаваемых между двумя защищенными сегментами разделенной ЛВС. Управление параметрами КШ осуществляется из той ЛВС, в которой установлена программа управления и на криптошлюзе которой установлен центр управления сетью.

Защищенная корпоративная VPN-сеть (рис. 2) предполагает, что защищаемые сегменты сети предприятия объединены между собой через каналы передачи данных сети общего пользования (выделенные каналы различной пропускной способности, в том числе сеть Internet). В этом случае обеспечивается:

• шифрование и имитозащита данных, передаваемых по каналам связи;
• аутентификация удаленных абонентов;
• фильтрация входящих и исходящих *IP*-пакетов;
• скрытие внутренней структуры каждого защищаемого сегмента сети;
• распределение и управление сменой ключей шифрования.

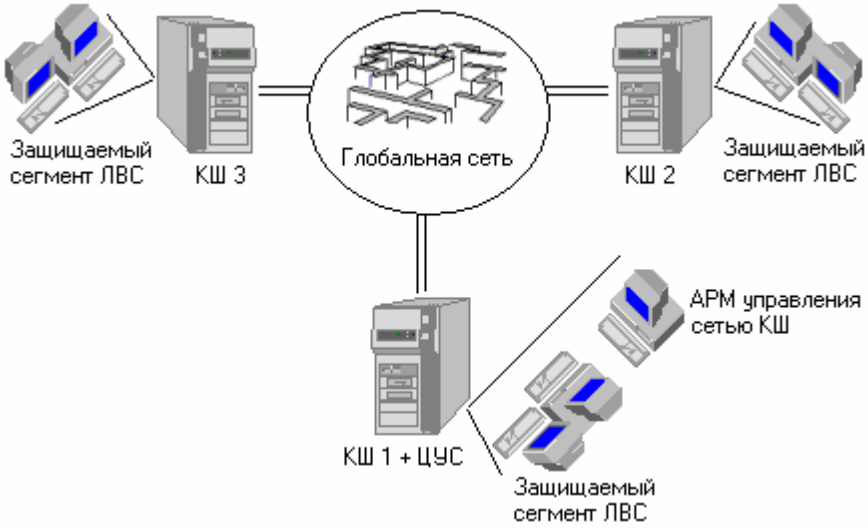


Рис. 2. Защищенная корпоративная сеть

Для централизованного управления работой КШ (настройка, контроль состояния, распределение ключей шифрования и т.д.) используются центр управления сетью и программа управления. Центр управления сетью устанавливается на одном из криптошлюзов сети. Программа управления может быть установлена на компьютерах внутри защищаемых центром управления сегментов сети. Оповещение администратора о попытках НСД осуществляется на АРМ управления сетью. Шифрование передаваемой информации для пользователей VPN является прозрачным.

Передача ключей на КШ с ЦУС производится по защищенному каналу связи (на ключе связи с ЦУС). В качестве ключевого носителя для ключа связи с ЦУС используется дискета. Ключи

парной связи хранятся на диске в зашифрованном виде (на ключе хранения). Ключ хранения находится в защищенной энергонезависимой памяти ЭЗ “Соболь”. Для защиты соединения между управляющей консолью и ЦУС используется специальный административный ключ. Этот ключ хранится на ключевом диске администратора системы. Плановая смена ключей на КШ осуществляется из ЦУС по каналу связи в защищенном виде на ключе связи с ЦУС.

Криптографический шлюз представляет собой специализированное программно-аппаратное устройство, обеспечивает:

• прием и передачу пакетов по протоколам семейства TCP/IP (статическая маршрутизация);
• шифрование передаваемых и принимаемых IP-пакетов;
• сжатие защищаемых данных; защиту данных от искажения ;
• фильтрацию IP-пакетов в соответствии с заданными правилами фильтрации;
• скрытие внутренней структуры защищаемого сегмента сети;
• криптографическую аутентификацию удаленных абонентов;
• периодическое оповещение ЦУС о своей активности;
• оповещение администратора (в реальном режиме времени) о событиях, требующих оперативного вмешательства;
• идентификацию и аутентификацию администратора при запуске КШ (средствами ЭЗ “Соболь”).

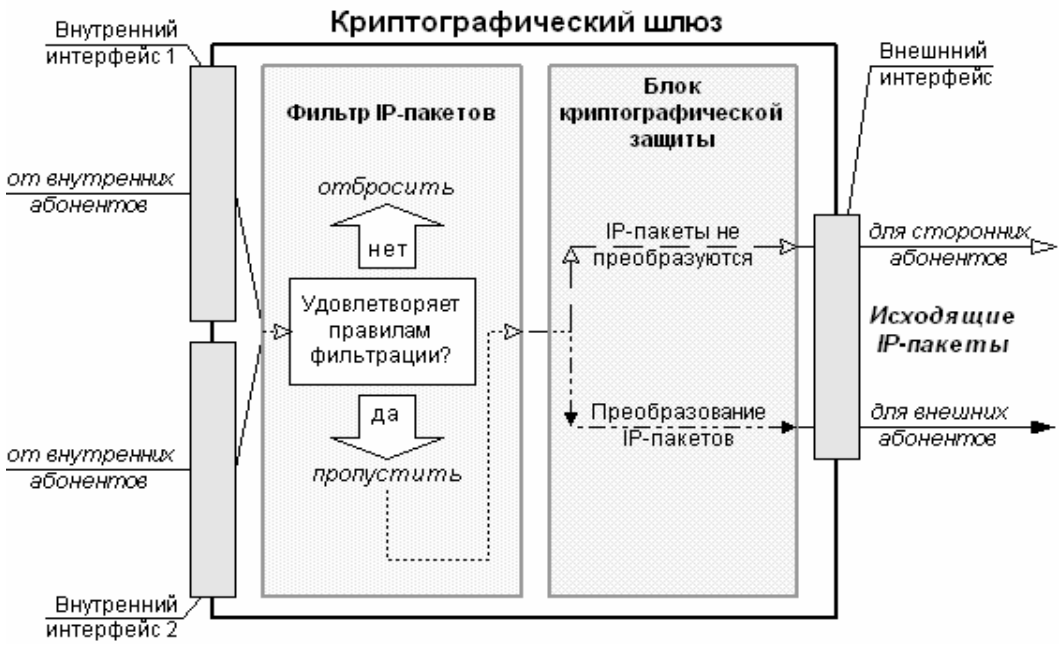


Рис. 3. Обработка исходящих IP-пакетов

Обработка исходящих IP-пакетов представлена на рис. 3. Все IP-пакеты, поступившие от внутренних абонентов защищаемого сегмента, вначале подвергаются фильтрации. Фильтрация IP-пакетов осуществляется в соответствии с установленными администратором правилами на основе IP-адресов отправителя и получателя, допустимых значений полей заголовка, используемых портов UDP/TCP и флагов TCP/IP-пакета. Если пакет не удовлетворят правилам фильтрации, он отвергается. Отправитель пакета получает ICMP-сообщение о недоступности абонента. При установке КШ автоматически генерируются правила, необходимые для обеспечения защищенного взаимодействия с ЦУС, корректной работы механизма маршрутизации пакетов, обработки управляющего трафика коммуникационного оборудования и обеспечения возможности начала работы VPN-функций без дополнительного конфигурирования. IP-пакеты, удовлетворяющие правилам фильтрации, обрабатываются блоком криптографической защиты и передаются на внешний интерфейс КШ. КШ-отправитель обеспечивает его сжатие, шифрование и имитозащиту, инкапсуляцию в новый IP-пакет, в котором в качестве IP-адреса приемника выступает IP-адрес КШ-получателя, а в качестве IP-адреса источника выступает IP-адрес КШ-отправителя. IP-пакеты, адресованные абонентам, внешним по отношению к VPN-сети (Web-сайты, ftp-серверы),

передаются в открытом виде. Это позволяет использовать КШ при доступе к общедоступным ресурсам сетей общего пользования в качестве межсетевого экрана пакетного уровня.

Входящие IP-пакеты от открытых абонентов блоком криптографической защиты не обрабатываются и поступают непосредственно в фильтр IP-пакетов. Для пакетов, полученных от абонентов VPN, блок криптографической защиты осуществляет проверку целостности пакетов и расшифровывает их, после чего пакеты поступают в фильтр IP-пакетов. Если целостность пакета нарушена, то пакет отбрасывается без расшифрования и без оповещения отправителя пакета с генерацией сообщения о НСД. IP-пакеты, удовлетворяющие правилам фильтрации, передаются через внутренний интерфейс внутренним абонентам.

ЛАБОРАТОРНАЯ РАБОТА№12

ТЕМА: Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы исходящие от использования «электронной почты».

ЦЕЛЬ: ИЗУЧЕНИЕ СПОСОБОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВИРУСОВ НА ПРИМЕРЕ ПРОГРАММЫ АНТИВИРУС КАСПЕРСКОГО

Антивирус Касперского – это классическая защита компьютера от вирусов, троянских и шпионских программ, а также от любого другого вредоносного ПО.

Базовая защита:

* Комплексная защита от всех видов вредоносных программ
* Проверка файлов, почтовых сообщений и интернет-трафика
* Защита интернет-пейджеров (ICQ, MSN). * Автоматическое обновление баз

Предотвращение угроз:Проактивная защита от новых и неизвестных угроз, Поиск уязвимостей в ОС и установленном ПО. Блокирование ссылок на зараженные сайты.Защита конфиденциальных данных:Блокирование ссылок на фишинговые сайты

Доп. функции:Защита от вирусов, троянских программ и червей. Защита от шпионских и рекламных программ. Проверка файлов в автоматическом режиме и по требованию. Проверка почтовых сообщений (для любых почтовых клиентов). Проверка интернет-трафика (для любых интернет-браузеров). Защита интернет-пейджеров (ICQ, MSN). Проактивная защита от новых вредоносных программ. Проверка Java- и VisualBasic-скриптов

Предотвращение угроз. Поиск уязвимостей в ОС и установленном ПО. Анализ и устранение уязвимостей в браузере InternetExplorer. Блокирование ссылок на зараженные сайты. Распознавание вирусов по способу их упаковки. Глобальный мониторинг угроз (KasperskySecurityNetwork). Восстановление системы и данных:Возможность установки программы на зараженный компьютер. Функция самозащиты программы от выключения или остановки. Восстановление корректных настроек системы после удаления вредоносного ПО. Наличие инструментов для создания диска аварийного восстановления

После запуска приложения в системной панели появляется значок, вид которого зависит от состояния антивирусной защиты: включена ли постоянная защита и запущена ли проверка по требованию. Если постоянная защита включена, значок активен (красного цвета)  , если выключена - неактивен (серого цвета)  . Если запущена полная проверка компьютера, проверка отдельного файла, диска или выполняется анализ какого-либо объекта в режиме постоянной защиты, то на системной панели отображается мигающий значок  . При проверке входящей почты появляется значок  , а при ошибке запуска одной из задач постоянной защиты -  . Во время загрузки обновлений антивирусных баз и модулей приложения значок меняется на  .

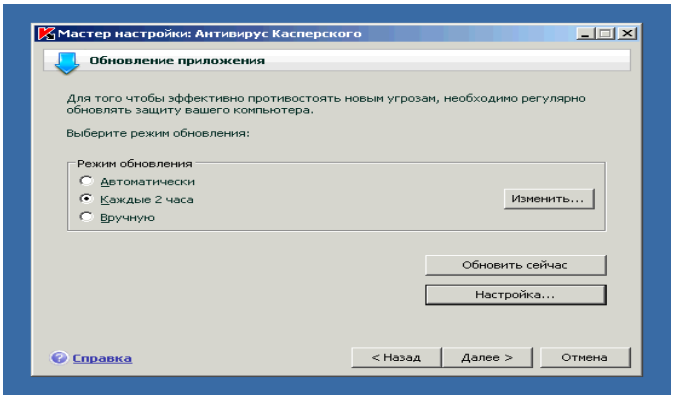
Настройка обновлений

1 способ. В процессе установки Антивируса Касперского версии 6.0 Мастер первоначальной настройки предлагает настроить обновление антивирусных баз. Вы можете выбрать один из трех режимов расписания обновления:

- **Автоматически** - процесс обновления самостоятельно проверяет свежие поступления на серверах обновлений **Лаборатории Касперского**, учитывая нагрузку на сервера. Специалисты **Лаборатории Касперского** рекомендуют использовать этот режим обновлений.
- **Каждый 2 часа** - Вы можете самостоятельно установить расписание обновлений. Возможно задать не только расписание дней, но и часы, минуты, недели, месяцы.
- **Вручную** - обновление стартует только по нажатии соответствующей кнопки в интерфейсе антивируса.

Нажав на кнопке**Обновить сейчас**, Вы можете немедленно обновить антивирусные базы еще до завершения процесса установки.

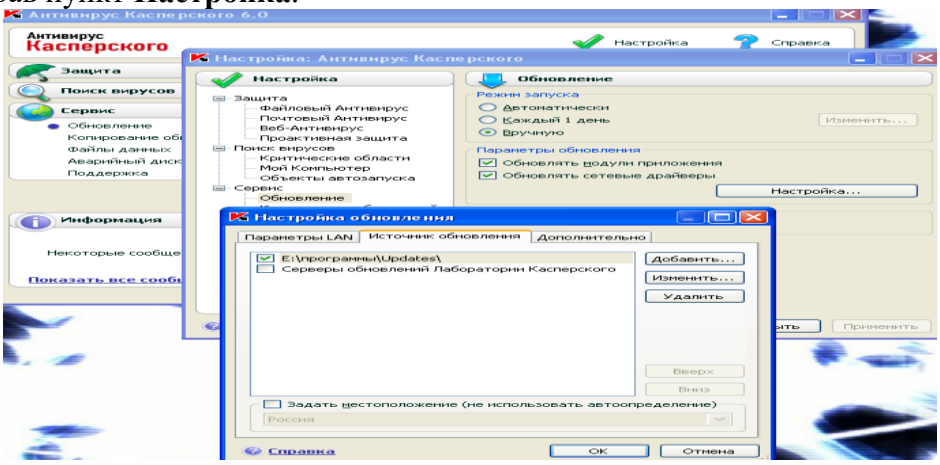
Нажав на кнопке **Настройка**, Вы можете задать вручную настройки прокси сервера, добавить или изменить источник обновления, а также задать учетную запись (логин\пароль) для процесса обновления.



Для начала выбираем Режим обновления (Автоматически, Каждые 2 часа или Вручную), затем задаем нужные нам настройки для случаев ручного Параметры LAN и источник обновления или периодической (график обновления) обновления

Задайте необходимые настройки и нажмите кнопку**Далее** для продолжения первоначальной настройки антивируса Касперского версии 6.0

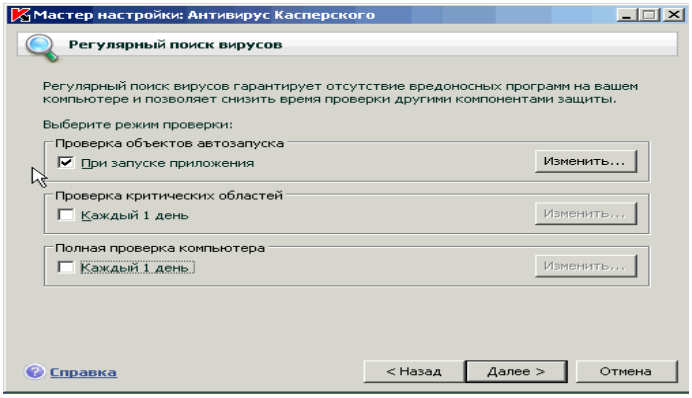
2 способ. Для обновления сигнатур антивирусной программы в процессе работы, войдем на вкладку **Сервис** выберем**Обновить** и укажем путь, откуда будем считывать новые сигнатуры выбрав пункт **Настройка**.



Настройка проверки компьютера

1 способ. В процессе установки Антивируса Касперского версии 6.0 Мастер первоначальной настройки предлагает настроить проверку областей компьютера:

- **Проверка объектов автозапуска** - проверка всех запускаемых файлов во время загрузки операционной системы **Windows**. По умолчанию расписание включено на режим **После запуска приложения**. Нажмите кнопку **Изменить** напротив этой опции для того, чтобы задать необходимое расписание.
- **Проверка критических областей** - проверка системных файлов, объектов автозапуска, системной памяти, загрузочных секторов дисков, системной памяти. По умолчанию расписание не включено. Нажмите кнопку **Изменить** напротив этой опции для того, чтобы задать необходимое расписание.
- **Полная проверка компьютера** - проверка всех файлов компьютера, а также критических областей на вирусы. По умолчанию расписание не включено. Нажмите кнопку **Изменить** напротив этой опции для того, чтобы задать необходимое расписание.



Задайте необходимые настройки для системных задач проверки **Объектов автозапуска**, **Критических областей** и **Моего компьютера** и нажмите кнопку**Далее** для продолжения первоначальной настройки антивируса Касперского версии 6.0

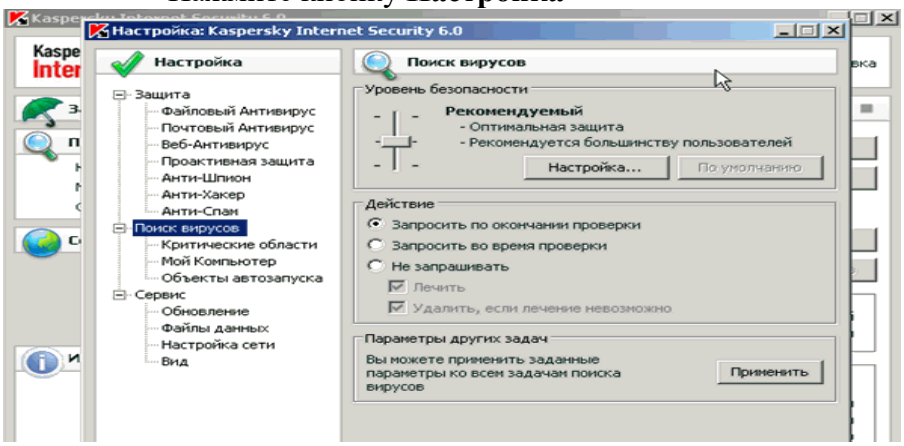
2 способ. В антивирусе Касперского версии 6.0 системные задачи удалить нельзя. Их можно только остановить, запустить или приостановить

- **Критические области** - проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные сектора дисков, системные каталоги ***Windows*** и ***system32***. Цель задачи - быстрое обнаружение в системе активных вирусов, без запуска полной проверки компьютера.
- **Мой Компьютер** - поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.
- **Объекты автозапуска** - проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

Настройки можно задать как для каждой задачи отдельно, так и для всех задач вместе.

Для того, чтобы задать настройки для всех задач вместе, необходимо сделать следующее:

- Откройте главное окно антивируса Касперского версии 6.0
- Выберите раздел **Поиск Вирусов**
- Нажмите кнопку **Настройка**



В главном окне настроек можно изменить следующие параметры:

- **Уровень безопасности** - выбрать один из трех уровней безопасности, установить пользовательский уровень безопасности, установить уровень безопасности по умолчанию
- **Действие над объектом** - запросить по окончании проверки, запросить во время проверки или не запрашивать, а лечить или удалить, если лечение невозможно.
- **Параметры других задач** - применить заданные параметры для **Поиска Вирусов** к трем системным задачам **Критические области**, **Мой Компьютер**, **Объекты автозапуска**, а также к пользовательским задачам, если они были созданы ранее.

Настройка проактивной защиты

В процессе установки **Антивируса Касперского 6.0 MP1\6.0 MP2**, **KasperskyInternetSecurity 6.0 MP1\6.0 MP2** и **Антивируса Касперского 6.0 для WindowsWorkstations**

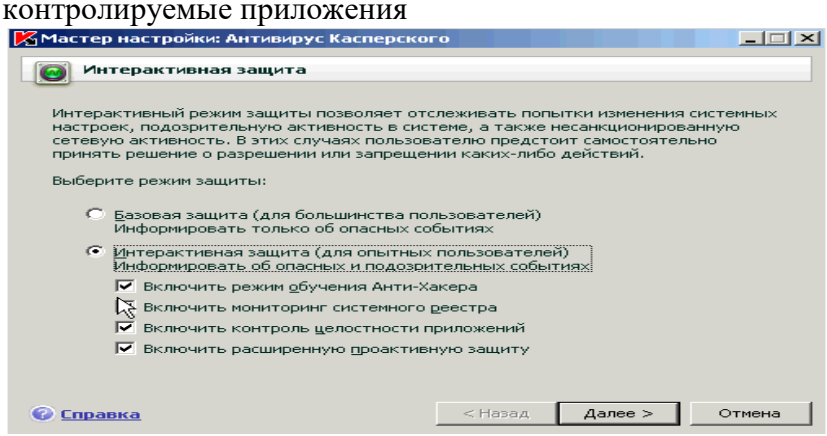
MP2\MP3 Мастер первоначальной настройки предлагает настроить компонент **Проактивная защита**:

Базовая защита – включены модули Анализ активности приложений и проверка VBA-макросов. Для Анализа активности включены функции:

- опасная активность (анализ поведения приложения в системе)
- внедрение в процесс (invaders)
- появления скрытого процесса (rootkit)
- подозрительные значения в реестре
- подозрительная активность в системе
- обнаружение клавиатурных перехватчиков

Интерактивная защита - расширенные модули включаются по желанию пользователя, а именно:

- Режим обучения Анти-хакера. По умолчанию Анти-хакер работает в режиме Минимальная защита. В режиме Минимальная Защита Анти-хакер использует предустановленные правила для приложений и пакетов, созданные специалистами Лаборатории Касперского на основе многолетнего опыта работы. В режиме обучения Анти-хакер позволяет пользователю самостоятельно разрешать или запрещать доступ приложеням, устанавливающимсоедининение с Интернет.
- Мониторинг системного реестра позволяет контролировать пользователю любое изменение в системном реестре операционной системы Windows.
- Контроль целостности приложений отслеживает попытки загрузки модулей в контролируемые приложения

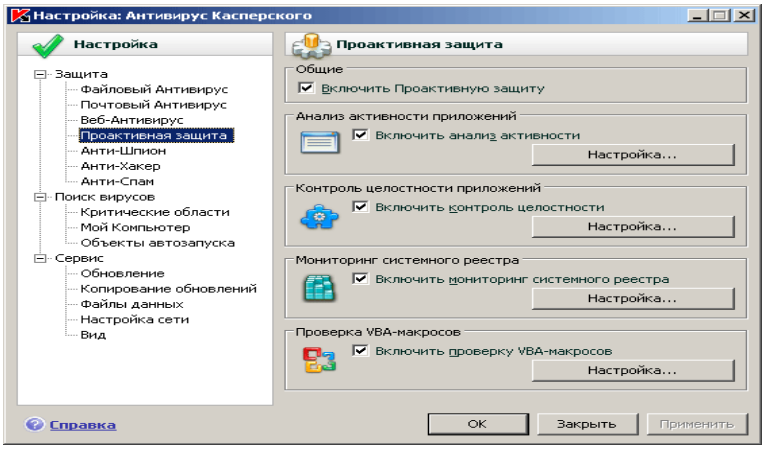


Расширенная проактивная защита включает для модуля Анализ активности приложений дополнительные функции:

- запуск браузера с параметрами
- внедрение оконных перехватчиков.

Выберите необходимый тип защиты для компонента **Проактивная защита** и нажмите кнопку**Далее** для продолжения первоначальной настройкиантивируса Касперского версии 6.0

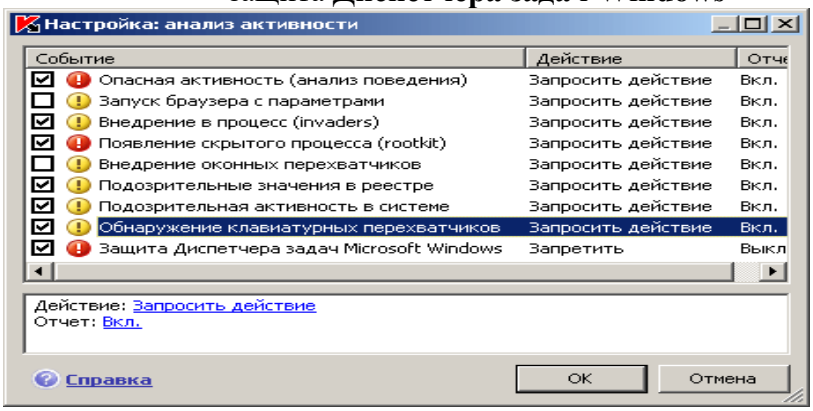
С каждым днем вредоносных программ становится все больше, они усложняются, комбинируя в себе несколько видов, методы распространения становятся все более сложными для обнаружения. Для того чтобы обнаружить новую вредоносную программу еще до того, как она успеет нанести вред, специалистами **Лабораторией Касперского** разработан специальный компонент – **Проактивная защита**. Он основан на контроле и анализе поведения всех программ, установленных на вашем компьютере. На основании выполняемых действий Антивирус Касперского версии 6.0 принимает решение: является программа опасной или нет. Таким образом, Ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.



Возможности компонента **Проактивная защита**:

анализ активности приложений: осуществляет контроль:

- опасная активность процессов
- запуск браузера с параметрами
- внедрение в процесс(**invaders**)
- появление скрытого процесса (**rootkit**) в системе
- внедрения оконного перехватчика
- подозрительные значения в реестре
- подозрительная активность в системе
- обнаружение клавиатурных перехватчиков
- защита **Диспетчера задач Windows**



Контроль Опасной активности: анализирует поведение всех процессов, запущенных в системе, сохраняя все изменения, производимые в файловой системе и реестре. При выполнении некоторым приложением набора подозрительных действий выдаётся предупреждение пользователю об опасности данного процесса.

Откат изменений после определения опасной активности в системе: технология, позволяющая восстанавливать систему после вредоносных действий, возвращая ее к незараженному состоянию.

Контроль запуска браузера с параметрами: позволяет перехватить скрытый запуск браузера с передачей ему параметров, что может быть использовано вредоносными программами.

Контроль внедрения кода в чужые процессы: позволяет перехватить все возможности внедрения программного кода в чужие процессы.

Технология борьбы с руткитами (контроль появления скрытого процесса): позволяет обнаруживать большинство из реализаций современных руткитов, которые могут скрывать от пользователя файлы, папки и ключи реестра, скрывать запущенные программы, системные службы, драйверы и сетевые соединения, скрывать сетевую активность.

Контроль внедрения оконного перехватчика: перехватывает попытку внедрения динамической библиотеки во все активные процессы в системе.

Подозрительные значения в реестре: позволяет перехватить попытку создания «скрытых» ключей в реестре, не отображаемых обычными программами (типа regedit).

Подозрительная активность в системе: отслеживает большое число различных изменений в системе, указывающих на присутствие активного вредоносного кода.

Обнаружение клавиатурных перехватчиков: отслеживает перехваты вредоносными программами информации, вводимой с клавиатуры.

Защита Диспетчера задач MicrosoftWindows: позволяет защитить **Диспетчер задач** от внедрения вредоносных модулей, деятельность которых направлена на блокирование работы **Диспетчера**.

Контроль целостности приложений (монитор приложений): позволяет задавать ряд приложений, для которых будет контролироваться компонентный состав.

Контроль системного реестра (монитор реестра): контролирует изменения ключей реестра. Содержит предустановленный список из 6 групп критических ключей. Также пользователь может добавить свои группы ключей и настроить правила доступа к ним для различных приложений.

Проверка VBA-макросов: Проверка опасных макросов **VisualBasicforApplication**.

ЛАБОРАТОРНАЯ РАБОТА №13
ТЕМА: Исследование методов тестирования и контроля защищенных систем радиосвязи

Оценка качества функционирования оборудования, обеспечивающего тракт звукового сигнала

Качество функционирования испытуемого оборудования при работе тракта звукового сигнала оценивают методом наводки звукового сигнала, либо методом оценки искажений звукового сигнала.

Оценка тракта звукового сигнала методом наводки звукового сигнала

Данным методом испытывают лишь оборудование, предназначенное для передачи речевых сигналов.Тракты звукового сигнала должны функционировать.Для создания линии связи применяют соответствующую испытательную систему. Параметры полезных радиочастотных сигналов, подаваемых на испытуемое оборудование, должны быть установлены по согласованию между испытательной лабораторией и изготовителем. Испытания радиооборудования в режиме радиопередачи (радиоприема) проводят в следующем порядке:

- устанавливают максимальную мощность радиопередатчика;
- устанавливают и регистрируют до начала серии испытаний опорные уровни выходного звукового сигнала при передаче по линии «вверх» и по линии «вниз» с использованием измерительных приборов, как показано на рисунке 1.

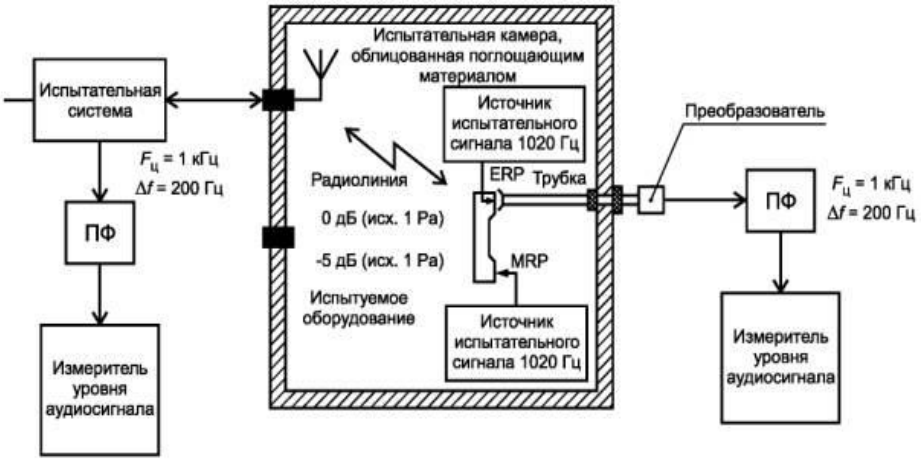


Рисунок 1 - Схема установки опорных уровней звукового сигнала

ПФ - полосовой фильтр; *F*ц - центральная частота полосы пропускания фильтра; Δ*f* - полоса пропускания фильтра; ERP - опорная точка уха; MRP - опорная точка рта

1 Положение испытуемого оборудования показано при установлении уровня опорного сигнала при передаче по линии «вверх».

2 Если испытуемое оборудование имеет громкоговоритель, опорный уровень должен быть равен 5,0 дБ (исх. 1 Ра) на частоте 1020 Гц.

Опорный уровень должен быть равен 0 дБ (исх. 1 Ра) на частоте 1020 Гц в опорной точке уха или 5,0 дБ (исх. 1 Ра) на громкоговорителе при передаче «вниз» и минус 5 дБ (исх. 1 Ра) на частоте 1020 Гц в опорной точке рта или у микрофона при передаче «вверх». Номинальные значения акустических сигналов, необходимые при проведении испытаний, могут быть адаптированы к оборудованию TETRA различных видов и к разным схемам подачи звуковых сигналов;

- оценивают уровень выходного звукового сигнала испытуемого оборудования, наведенного в результате воздействия помех при передаче по линии «вниз» путем измерения звукового давления, как показано на рисунке 2. При этом должны быть приняты меры для исключения воздействия внешнего акустического шума на микрофон испытуемого оборудования;

- измеряют на выходе испытательной системы уровень звукового сигнала испытуемого оборудования, наведенного в результате воздействия помех при передаче по линии «вверх» по каналу звукового сигнала испытуемого оборудования.

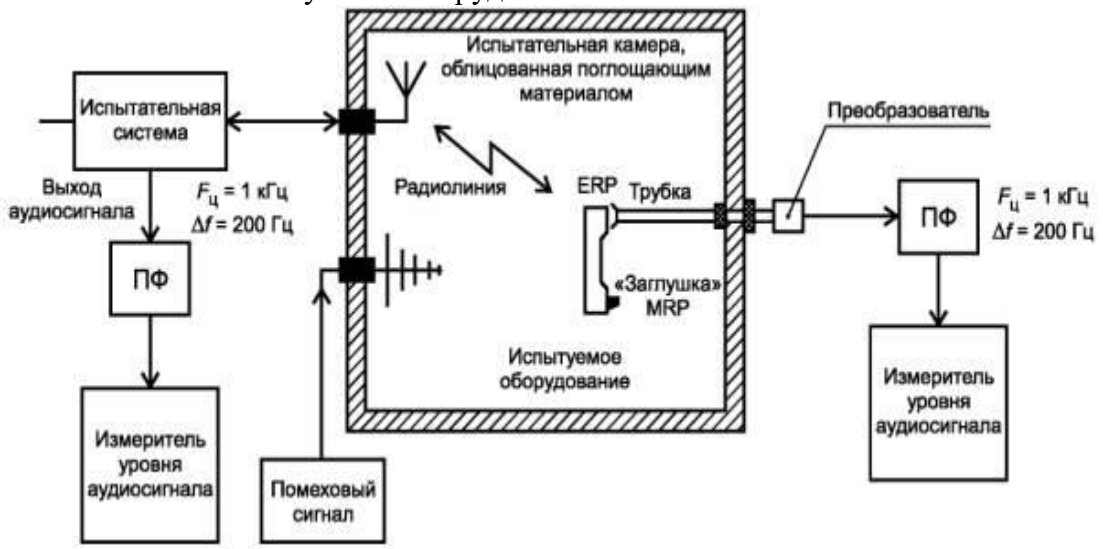


Рисунок 2 - Схема испытаний при наводке звукового сигнала

Оценка тракта звукового сигнала методом оценки искажения звукового сигнала

Данным методом испытывают лишь оборудование, предназначенное для передачи речевых сигналов.Тракты звукового сигнала должны функционировать.

Для создания линии связи применяют соответствующую испытательную систему. Параметры полезных радиочастотных сигналов, подаваемых на испытуемое оборудование, должны быть установлены по согласованию между испытательной лабораторией и изготовителем. Испытания радиооборудования проводят в следующем порядке:

- устанавливают максимальную мощность радиопередатчика;

- устанавливают линию связи между испытуемым оборудованием и испытательной системой. В испытательной системе сигнал при передаче по линии «вверх», принимаемый от испытуемого оборудования, возвращается по петле кольцевой проверки на испытуемое оборудование в качестве сигнала, передаваемого «вниз». Петля проверки в испытательной системе должна сохранять возвращаемый сигнал в цифровом формате или так, чтобы он оставался неизменным;

- сигнал частотой 1020 Гц, уровень которого находится в пределах динамического диапазона звуковой схемы микрофона, подают в опорную точку рта;

- звуковой сигнал после петли проверки в испытательной системе получают в опорной точке уха с помощью преобразователя. Сигнал преобразователя посредством неметаллической акустической трубки передают на анализатор искажений звукового сигнала, находящийся вне помещения для испытаний. При этом необходимо принять меры для исключения воздействия внешнего акустического шума на микрофон испытуемого оборудования и преобразователь, подключаемый к акустической трубке.

ЛАБОРАТОРНАЯ РАБОТА №14

ТЕМА: Исследование методов защиты телетрафика в сетях и систем радиосвязи

Под ***аналоговым скремблированием*** подразумевается преобразование исходного речевого сигнала с целью минимизации признаков речевого сообщения, в результате которого этот сигнал становится неразборчивым и неузнаваемым. При этом он занимает такую же полосу частот спектра, как и исходный сигнал. Необходимым свойством такого преобразования является возможность обратного преобразования для восстановления речевого сигнала на приемной стороне.

Технические средства, обеспечивающие защиту информации аналоговыми методами, называются ***скремблерами***. Иногда их называют также маскираторами речи. Как правило, в сигнале, закрытом с помощью аналогового скремблера, все-таки сохраняются отдельные признаки открытого речевого сообщения.

В целом, аналоговые методы защиты информации обеспечивают меньшую степень закрытия речевых сигналов по сравнению с цифровыми, однако при практической реализации они, как правило, более просты, дешевы, а также характеризуются достаточно высоким качеством восстановленного речевого сигнала.

При скремблировании возможно преобразование речевого сигнала по трем параметрам: амплитуде, частоте и времени. Однако в системах подвижной радиосвязи практическое применение нашли в основном частотные и временные преобразования сигнала, а также их комбинации. Возможные помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, в связи с чем амплитудные преобразования при скремблировании практически не применяются.

При ***частотных преобразованиях сигнала*** в средствах подвижной радиосвязи чаще всего используются следующие виды скремблирования:

- частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра);
- разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра в каждом относительно средней частоты поддиапазона;
- разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки.

При ***временных преобразованиях*** производится разбиение сигнала на речевые сегменты и их перестановки во времени. При этом, в основном, используются два способа закрытия:

- инверсия по времени сегментов речи;
- временные перестановки сегментов речевого сигнала.

Комбинированные методы преобразования сигнала предполагают использование одновременно нескольких различных способов скремблирования (как частотных, так и временных), число которых ограничивается, как правило, возможностями технической реализации аналоговых скремблеров.

Основными техническими характеристиками аналоговых скремблеров являются уровень закрытия информации, остаточная разборчивость и качество восстановления сигнала.

Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является ***уровень закрытия информации***. Следует отметить, что, если для сложных цифровых систем передачи речи и данных понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил.

В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать количество ключевых параметров и количество возможных ключей скремблера.

Под ***ключевым параметром аналогового скремблера*** обычно понимают какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне.

Ключом аналогового скремблера (по аналогии с цифровыми системами шифрования), как правило, называют конкретное секретное состояние некоторых параметров преобразования речевого сигнала. ***Количество ключей*** скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний этого параметра, для скремблеров с несколькими ключевыми параметрами - количеством возможных комбинаций значений этих параметров (как правило, произведением чисел состояний всех ключевых параметров).

Качество восстановления сигнала определяется искажениями сигнала при его частотных или временных преобразованиях. Фактически, эта характеристика отражает разборчивость и узнаваемость восстановленной речи. Приемлемым или коммерческим качеством восстановленной на приемном конце речи считается такое, когда слушатель без усилий может определить голос говорящего и смысл произносимого сообщения.

Наилучшим качеством восстановления сигнала обладают частотные инверторы, которые практически не ухудшают разборчивость и узнаваемость речи при правильной реализации. Более сложные методы частотных преобразований могут вносить некоторые искажения в речевой сигнал. Реализация высокого качества восстановления речи при временных преобразованиях требует достаточно сложной обработки.

Под ***остаточной разборчивостью*** понимают процент восстановленных фрагментов скремблированного речевого сигнала при прослушивании переговоров с помощью обычных УКВ-приемников или радиостанций, не оснащенных аналогичным скремблером.

Следует отметить, что подавляющее большинство известных аналоговых речевых скремблеров в той или иной мере сохраняют остаточную разборчивость. В прослушиваемом речевом сигнале, защищенном скремблером, сохраняется информация о темпе речи, улавливаются паузы. При несложных способах защиты опытный оператор может разобрать (в зависимости от наличия сведений о тематике ведущихся переговоров) от 10 до 50 % передаваемой информации.

При ***частотной инверсии*** преобразование спектра речевого сигнала эквивалентно повороту частотной полосы сигнала вокруг некоторой средней частоты ($F_и$). Принцип данного преобразования сигнала показан на рис. 1: а) - исходный спектр сигнала, б) - спектр сигнала после инверсии.

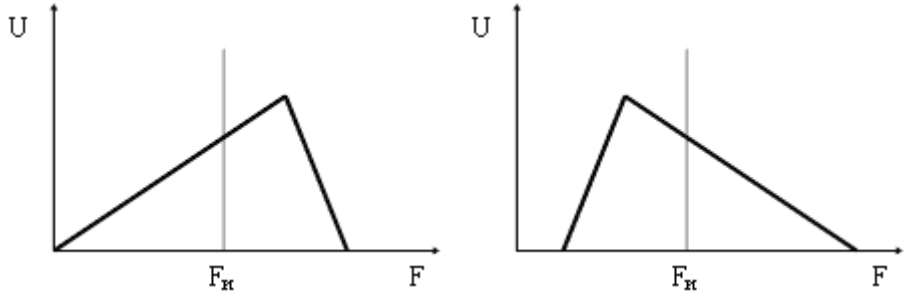


Рис. 1. Принцип работы частотного инвертора речевого сигнала.

Несколько более сложный по сравнению с частотной инверсией способ преобразования сигнала обеспечивает скремблер с ***разбиением полосы речевого сигнала на поддиапазоны с частотной инверсией сигнала в каждом поддиапазоне*** (полосно-сдвиговый инвертор). Обычно используется разбиение полосы на 2 поддиапазона. Принцип такого частотного преобразования для 2-х поддиапазонов показан на рис. 2, где а) - исходный спектр сигнала; б) - спектр сигнала после преобразования, $F_р$ - частота разбиения спектра сигнала; $F_{и1}$, $F_{и2}$ - частоты инверсии 1-го и 2-го поддиапазонов.

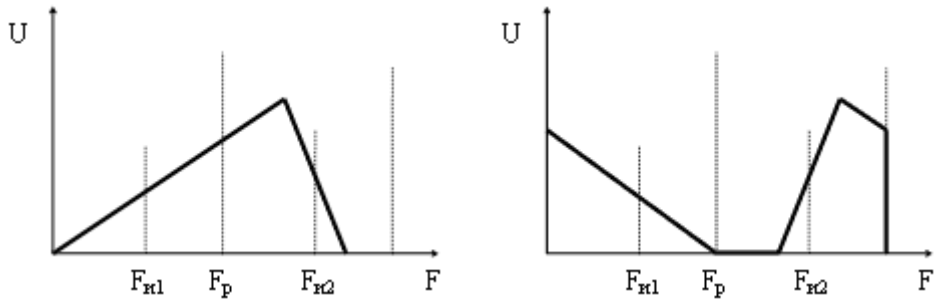


Рис. 2. Принцип работы полосно-сдвигового инвертора речевого сигнала при разбиении спектра сигнала на 2 поддиапазона.

Полосовые скремблеры используют способ ***разбиения полосы речевого сигнала на несколько поддиапазонов с частотными перестановками этих поддиапазонов***. Принцип работы полосового скремблера с разбиением спектра сигнала на 4 полосы показан на рис. 3.

Полосовой скремблер может быть реализован на основе быстрого преобразования Фурье (БПФ). В таком скремблере на передающей стороне производится прямое БПФ, частотная перестановка полос, а затем - обратное БПФ. На приемной стороне осуществляются аналогичные преобразования с обратной частотной перестановкой полос.

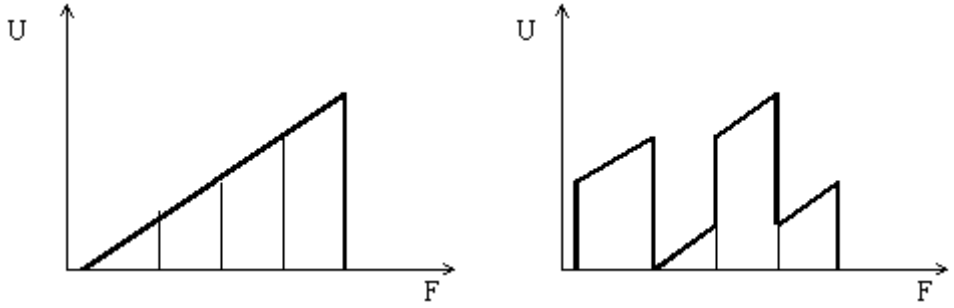


Рис. 3. Принцип работы 4-х полосового скремблера.

В скремблерах с БПФ возможно достичь высокой степени защиты информации за счет увеличения количества перемешиваемых полос, однако на практике этот метод скремблирования в подвижной радиосвязи применяется редко в связи со сложностями технической реализации. Кроме этого, скремблеры с БПФ вносят в канал связи временную задержку.

Простейшим видом временного преобразования является ***временная инверсия***, при которой исходный сигнал делится на последовательность временных сегментов и каждый из них передается инверсно во времени - с конца к началу. Принцип работы временного инвертора показан на рис. 4.

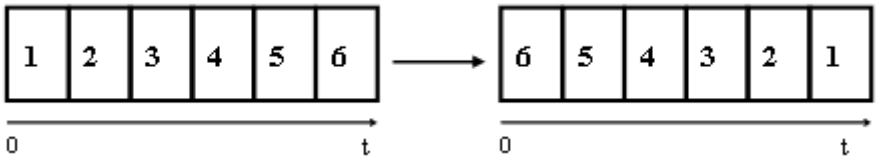


Рис. 4. Принцип работы временного инвертора.

В ***скремблере с временными перестановками*** речевой сигнал делится на временные кадры, каждый из которых в свою очередь подразделяется на сегменты, а затем сегменты речевого сигнала подвергаются перестановке. Принцип работы такого скремблера *с фиксированным окном* и числом временных сегментов в кадре, равном 6, показан на рис. 5.

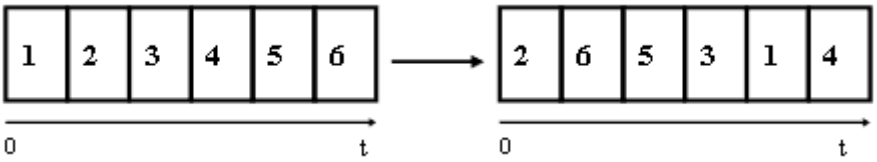


Рис. 5. Принцип работы скремблера с временными перестановками.

Все рассмотренные выше скремблеры предполагают фиксированные параметры преобразования сигнала (фиксированные ключи) в течение передачи речевого сообщения и поэтому называются ***статическими***.

Дополнительное повышение уровня закрытия информации может быть обеспечено *изменением параметров преобразования сигнала во времени.* Такие скремблеры называются***динамическими,*** а в современной практике их принято обозначать термином ***роллинговые*** скремблеры (от англ. *rolling*).

Динамические скремблеры, как правило, существенно дороже скремблеров с фиксированными параметрами преобразования сигнала, сильнее влияют на характеристики радиосредств и требуют начальной синхронизации. Однако их применение действительно затрудняет возможности перехвата переговоров, в особенности в реальном масштабе времени.

Это объясняется тем, что изменение ключевых параметров во времени теоретически делает возможным резкое увеличение количества ключей, под которыми для роллинговых скремблеров обычно понимают некоторое значение, определяющее порядок изменения параметров преобразования сигнала. Например, ключом может быть начальное значение генератора псевдослучайной последовательности, в соответствии с которой меняется определенный ключевой параметр.

Временные преобразования сигнала в сочетании с изменением ключевых параметров во времени достаточно сложны для реализации и требуют относительно длительной синхронизации, поэтому они пока не нашли свое применение в роллинговых скремблерах. Для способов частотного преобразования сигнала изменяемыми ключевыми параметрами могут быть частота инверсии (для частотного инвертора), частота разбиения полосы сигнала (для полосно-сдвигового инвертора), комбинация частотной перестановки поддиапазонов сигнала (для полосового скремблера). Большинство известных моделей роллинговых скремблеров используют наиболее простой принцип спектрального преобразования - частотный инвертор с изменением частоты инверсии сигнала во времени.

Различие скремблеров состоит в числе частот инверсии, скорости их изменения и количестве ключей, определяющих длительность перебора возможных комбинаций изменяемых параметров без их повторения.

Сравнение

Обычно пользователя больше всего интересует вопрос, какой скремблер обеспечит наибольшую защиту информации. Следует сказать, что представленные аналоговые скремблеры не могут обеспечить гарантированную стойкость информации, поэтому их нельзя рассматривать как средства криптографической защиты информации (СКЗИ). Речь может идти только о затруднении прослушивания конкурентом или злоумышленником переговоров, ведущихся с помощью радиосредств, оснащенных скремблерами, в реальном масштабе времени. Как уже было сказано, некоторое представление о степени закрытия информации может дать количество ключевых параметров и количество ключей. Причем следует рассматривать эти параметры в совокупности, при равном количестве ключей преимущество имеют скремблеры с бóльшим количеством ключевых параметров. Рассмотрим с этой точки зрения представленные виды скремблеров.

Для *частотного инвертора* единственным ключевым параметром является значение частоты инверсии сигнала. Размерность этого параметра, т. е. число возможных значений частот инверсии (число ключей) с ощутимыми искажениями, возникающими при прослушивании на соседней частоте, не превышает 20-30. Для перехвата переговоров, ведущихся с помощью радиосредств, оснащенных частотным инвертором, достаточно иметь аналогичную радиостанцию или сканирующий приемник с возможностью подбора частоты инверсии.

В *полосно-сдвиговых инверторах* в качестве основного ключевого параметра выступает частота разбиения полосы речевого сигнала $F_р$, размерность которой сопоставима с размерностью ключевого параметра частотного инвертора. Если частота разбиения является единственным ключевым параметром, то данный способ аналогового скремблирования обеспечивает закрытие речевой информации, сравнимое с частотной инверсией. В случае когда могут изменяться и

частоты инверсии в каждой из полос, число ключей, соответственно и уровень закрытия информации, увеличиваются.

В *полосовых скремблерах* ключевыми параметрами системы является число частотных полос и кодовая комбинация их перестановки. Реально число полос не превышает 4-х, поэтому число возможных комбинаций – 24 (одна из них не является перестановкой).

Скремблеры с временными перестановками имеют несколько ключевых параметров: длительность сегмента речи, длительность временного отрезка и правило перестановки временных отрезков в сегменте. Различные сочетания значений этих параметров могут дать возможность реализации нескольких сотен ключей.

Роллинговые скремблеры предоставляют возможность использования в сети радиосвязи такого количества ключевых комбинаций, которое может измеряться миллионами или даже миллиардами. При этом уровень защиты определяется количеством градаций параметра сигнала, длиной ключа, т. е. числом возможных комбинаций параметра, скоростью изменения параметра.

Однако повышение степени закрытия информации в гораздо большей степени зависит от количества градаций ключевого параметра (например, количества частот инверсии сигнала), чем от длины последовательности их перебора.

Следует отметить, что при низкой скорости изменения частоты инверсии (например, 1 раз в секунду) еще сохраняется возможность понимания какой-то части передаваемой информации при ее прослушивании с помощью радиостанции, оснащенной скремблером с фиксированной частотой инверсии. Однако при увеличении скорости до 5-10 раз в секунду возможность такого понимания резко снижается. Необходимость дальнейшего увеличения скорости смены параметра преобразования вызывает некоторые сомнения.

Перехват сообщений в реальном масштабе времени в каналах связи, защищенных с помощью скремблеров с параметрами преобразования, изменяемыми во времени, возможен при применении специальных технических средств, позволяющих сначала определить ключевую последовательность (т. е. правила изменения параметров преобразования сигнала), а затем подстроиться под найденную ключевую последовательность. Вместе с тем, это оборудование должно быть значительно сложнее по сравнению со средствами перехвата переговоров абонентов, радиостанции которых оснащены скремблерами с фиксированными параметрами.

ЛАБОРАТОРНАЯ РАБОТА№15
ТЕМА: МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ТЕЛЕФОННЫХ ЛИНИЙ
ЦЕЛЬ: ИЗУЧИТЬ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ТЕЛЕФОННЫХ ЛИНИЙ

Методы и средства защиты телефонных линий должны быть направлены на исключение:
• использования телефонных линий для прослушивания разговоров, ведущихся в помещениях, через которые проходят эти линии;
• прослушивания телефонных разговоров, ведущихся по данным телефонным линиям;
• несанкционированного использования телефонных линий для ведения телефонных разговоров.

При положенной трубке телефонный и микрофонный капсюли гальванически отключены
от телефонной линии, и информационные сигналы возникают в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ. Перехват возникающих в элементах звонковой цепи информационных сигналов возможен путем гальванического подключении к телефонной линии специальных высокочувствительных низкочастотных усилителей (рис.1). Однако вследствие малой амплитуды сигналов, дальность перехвата информации, как правило, не превышаем нескольких десятков метров.

Для повышения дальности перехвата информации низкочастотный усилитель подключают к линии через устройство анализа состояния телефонной линии, включаемое в разрыв телефонной линии (рис. 2). Данное устройство при положенной трубке телефонного аппарата отключает линию от АТС (сопротивление развязки составляет более 20 МОм), подключает специальный низкочастотный усилитель и переходит в режим анализа поднятия телефонной трубки и наличия сигналов вызова. При получении сигналов вызова или поднятии телефонной трубки устройство отключает специальный низкочастотный усилитель и подключает телефонный аппарат к линии АТС.

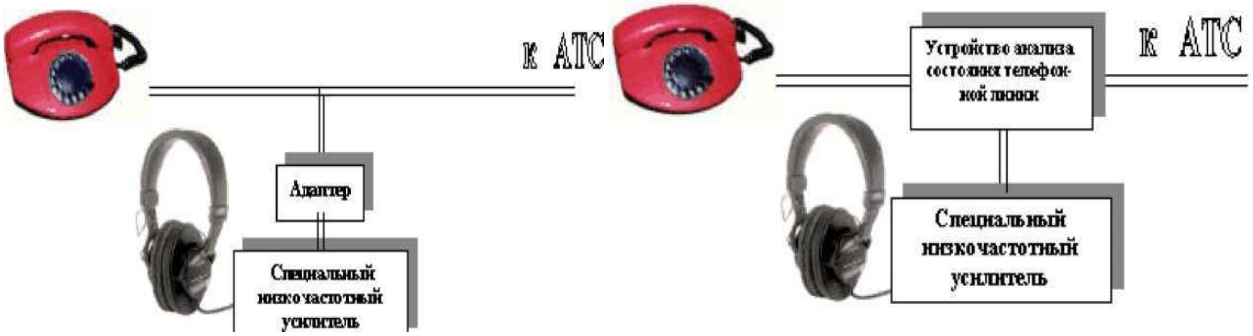


Рис. 1 Схема подключения специальных низкочастотных усилителей к телефонной линии через адаптер
Рис. 2 Схема подключения низкочастотного усилителя к телефонной линии через специальное устройство анализа состояния телефонной линии

Вследствие отключения телефонного аппарата от линии в момент съема информации значительно уменьшается уровень шумов в линии и, следовательно, повышается дальность перехвата информации.

Второй способ повышения дальности перехвата информации заключается в использовании метода “высокочастотного навязывания”, который может быть осуществлен путем контактного введения токов высокой частоты от генератора, подключенного в телефонную линию. Частота сигнала “навязывания” может составлять от 30 кГц до 10 МГц и более. Благодаря высокой частоте сигнал “навязывания” проходит не только в звонковую, но и в микрофонную и телефонную цепи и модулируется информационным сигналом, возникающим вследствие акустоэлектрических преобразований. В силу того, что нелинейные или параметрические элементы телефонного аппарата для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный речевым сигналом высокочастотный сигнал будет отражаться от нее

и распространяться в обратном направлении по линии. Отраженный высокочастотный сигнал принимается и обрабатывается специальным приемным устройством, также подключаемым к телефонной линии (рис. 3).

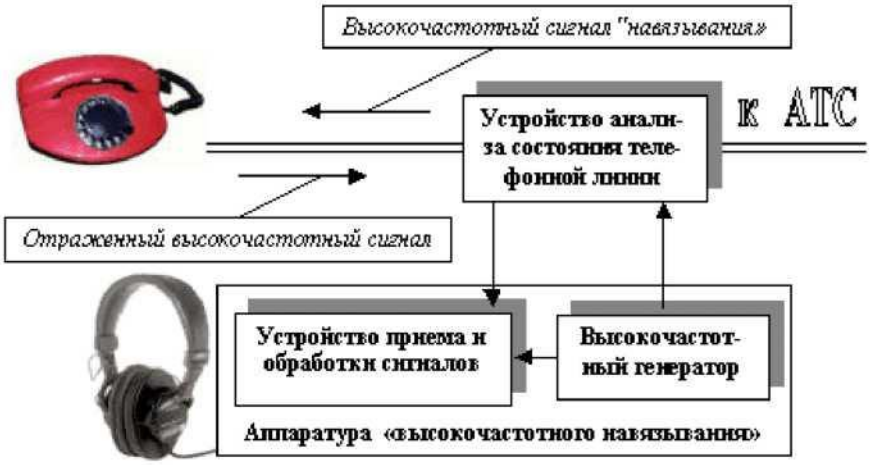


Рис.3 Схема реализации метода “высокочастотного навязывая”

Для защиты телефонного аппарата от утечки речевой информации по электроакустическому каналу используются как пассивные, так и активные методы и средства. К наиболее широко применяемым **пассивным методам защиты** относятся: • ограничение опасных сигналов; • фильтрация опасных сигналов; • отключение источников (преобразователей) опасных сигналов.

Наряду с электроакустическими каналами утечки информации для прослушивания разговоров в помещениях могут использоваться электронные устройства перехвата речевой (акустической) информации, использующие телефонную линию в качестве канала передачи информации. При этом передача информации может осуществляться как на низких (в речевом диапазоне частот), так и на высоких частотах (от 40 кГц до 10 МГц и более). Для передачи информации по телефонной линии на низких частотах используются микрофонные проводные системы и устройства типа “телефонное ухо”. Типовое электронное устройство перехвата информации включает: микрофон, микрофонный усилитель, электронный коммутатор и устройство анализа состояния телефонной линии (рис.4).

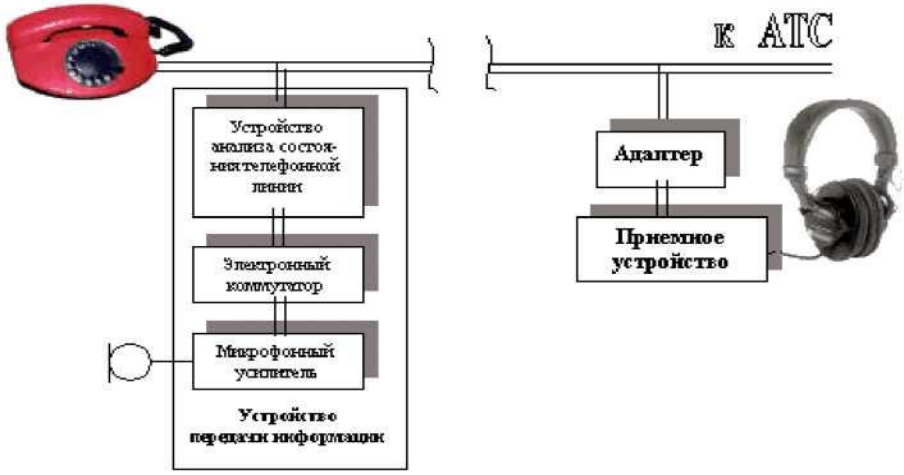


Рис. 4. Схема микрофонной проводной системы, использующей для передачи информации телефонную линию

Электронный коммутатор и устройство анализа состояния телефонной линии используются для исключения возможности обнаружения факта подключения закладного устройства к телефонной линии по наличию в ней посторонних сигналов при ведении телефонных разговоров. Устройство анализа контролирует состояние телефонной линии и при положенной телефонной трубке через электронный коммутатор подключает выход микрофонного усилителя к телефонной линии. При поднятии телефонной трубки микрофонный усилитель от телефонной

линии отключается. В качестве приемного устройства в системе могут использоваться низкочастотный усилитель или портативное устройство регистрации речевой информации (магнитофон, диктофон, устройства записи на основе использования цифровых методов звукозаписи), подключаемые к линии с помощью специального адаптера. Дальность передачи информации при использовании проводных микрофонных систем составлять несколько километров.

Схема перехвата информации с использованием устройств типа “телефонное ухо” показана на рис.5. В данной системе в качестве устройства дистанционного управления используется

обычный телефонный аппарат (возможно использование аппаратов сотовой связи). Принцип работы устройства передачи информации заключается в следующем. После набора номера “телефона-наблюдателя”, к линии которого подключено устройство, абонент переключает телефонный аппарат в тональный режим и осуществляет набор кодового числа. При отсутствии у телефонного аппарата режима тонового набора, для трансляции в линию кодированного звукового (тонального) сигнала используется специальное кодовое устройство (это устройство часто называют “бипером”). В момент передачи кодированного сигнала “бипер” подносится к микрофону телефонной трубки. Устройство анализа состояния линии закладки при приеме кодированного сигнала подавляет сигналы вызова, что обеспечивает скрытность работы устройства. При совпадении принятого кодового сигнала с записанным в память дешифратора, электронный коммутатор шунтирует телефонную линию сопротивлением 600 Ом. При этом АТС переключает “телефон-наблюдатель” на прием-передачу информации и в линию подается сигнал с выхода микрофонного усилителя, что обеспечивает звонящему абоненту возможность прослушивания разговоров, ведущихся в комнате, где установлено устройство. При поднятии трубки “телефона-наблюдателя” микрофонный усилитель от телефонной линии отключается.

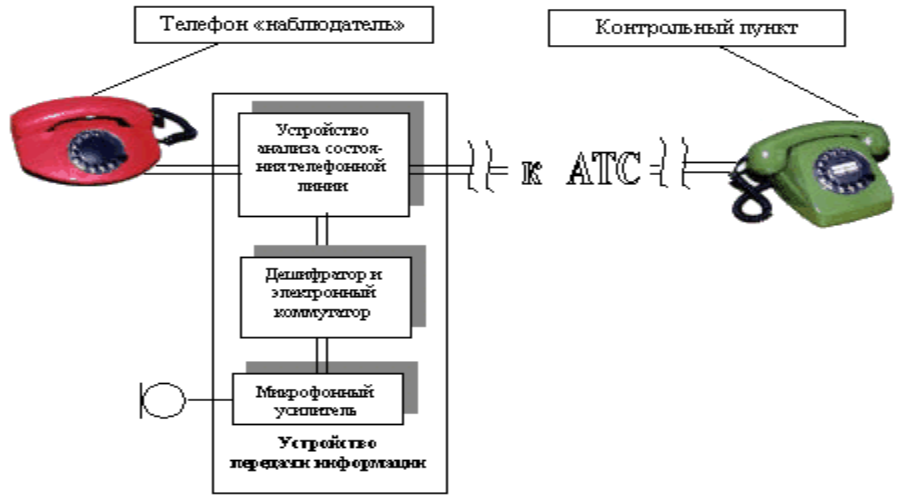


Рис. 5. Схема перехвата информации с использованием устройств типа “телефонное ухо”

В отличие от проводных микрофонных систем в системе перехвата информации с использованием устройств типа “телефонное ухо” дальность передачи информации практически не ограничена. Как правило, питание устройств передачи информации осуществляется от телефонной линии. Схема системы передачи информации по телефонной линии на высокой частоте представлена на рис. 6.. Фактически устройство представляет собой радиопередатчик, в качестве антенны которого используется телефонный провод. Наибольшая дальность передачи информации обеспечивается при использовании частот от 200 до 600 кГц. При передаче используется сигналы с частотной модуляцией. Дальность передачи информации при использовании подобных систем составлять

несколько километров.

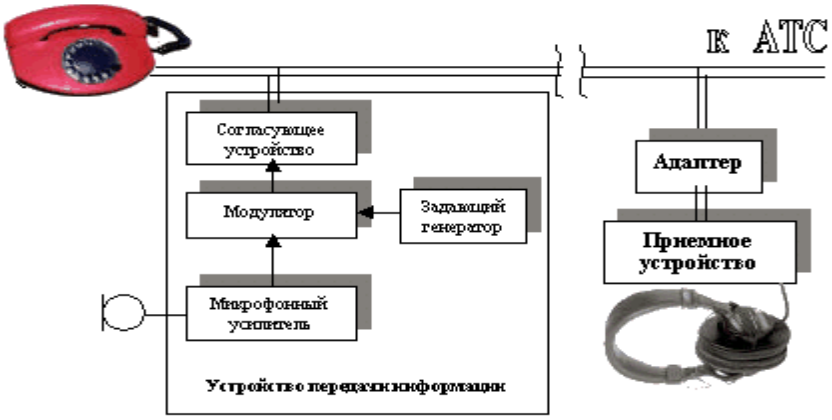


Рис. 6 Схема системы передачи информации по телефонной линии на высокой частоте

ЛАБОРАТОРНАЯ РАБОТА №16

ТЕМА: Мониторинг и диагностика средств защиты беспроводной локальной сети стандарта IEEE 802.11

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль — это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную. Процесс контроля работы сети обычно делят на два этапа — мониторинг и анализ.

На *этапе мониторинга* выполняется более простая процедура — процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап *анализа,* под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Классификация средств мониторинга и анализа

Все многообразие средств, применяемых для анализа и диагностики вычислительных сетей, можно разделить на несколько крупных классов.

- Агенты систем управления, поддерживающие функции одной из стандартных MIB (**MIB (ManagementInformationBase)** — база данных информации управления, используемая в процессе управления сетью в качестве модели управляемого объекта в архитектуре агент-менеджер) и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.
- Встроенные системы диагностики и управления (Embeddedsystems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.
- Анализаторы протоколов (Protocolanalyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, — обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические

условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

- Экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании NetworkGeneral. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.
- Оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.
  - Сетевые мониторы (называемые также сетевыми анализаторами) предназначены длятестирование кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика — средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т. п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех групп устройств данного класса, так как работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.
  - Устройства для сертификации кабельных систем выполняют сертификацию в соответствии с требованиями одного из международных стандартов на кабельные системы.
  - Кабельные сканеры используются для диагностики медных кабельных систем.
  - Тестеры предназначены для проверки кабелей на отсутствие физического разрыва. Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

Диагностика средств защиты беспроводной локальной сети

Любая методика тестирования сети существенно зависит от имеющихся в распоряжении системного администратора средств. По мнению некоторых администраторов, в большинстве случаев необходимым и достаточным средством для обнаружения дефектов сети (кроме кабельного сканера) является анализатор сетевых протоколов. Он должен подключаться к тому домену сети (collisiondomain), где наблюдаются сбои, в максимальной близости к наиболее подозрительным станциям или серверу

Если сеть имеет архитектуру с компактной магистралью (collapsedbackbone) и в качестве магистрали используется коммутатор, то анализатор необходимо подключать к тем портам коммутатора, через которые проходит анализируемый трафик. Некоторые программы имеют специальные агенты или зонды (probes), устанавливаемые на компьютерах, подключенных к удаленным портам коммутатора. Обычно агенты (не путать с агентами SNMP) представляют собой сервис или задачу, работающую в фоновом режиме на компьютере пользователя. Как правило, агенты потребляют мало вычислительных ресурсов и не мешают работе пользователей, на компьютерах которых они установлены. Анализаторы и агенты могут быть подключены к коммутатору двумя способами.

При первом способе анализатор подключается к специальному порту (порту мониторинга или зеркальному порту) коммутатора, если таковой имеется, и на него по очереди направляется трафик со всех интересующих портов коммутатора.

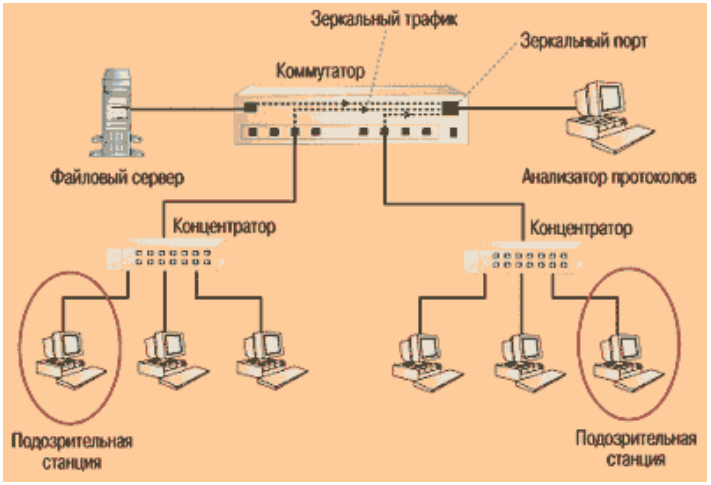


Рисунок – Первый способ подключения анализатора

Если в коммутаторе специальный порт отсутствует, то анализатор (или агент) следует подключать к портам интересующих доменов сети в максимальной близости к наиболее подозрительным станциям или серверу. Иногда это может потребовать использования дополнительного концентратора. Данный способ предпочтительнее первого. Исключение составляет случай, когда один из портов коммутатора работает в полнодуплексном режиме. Если это так, то порт предварительно необходимо перевести в полудуплексный режим.

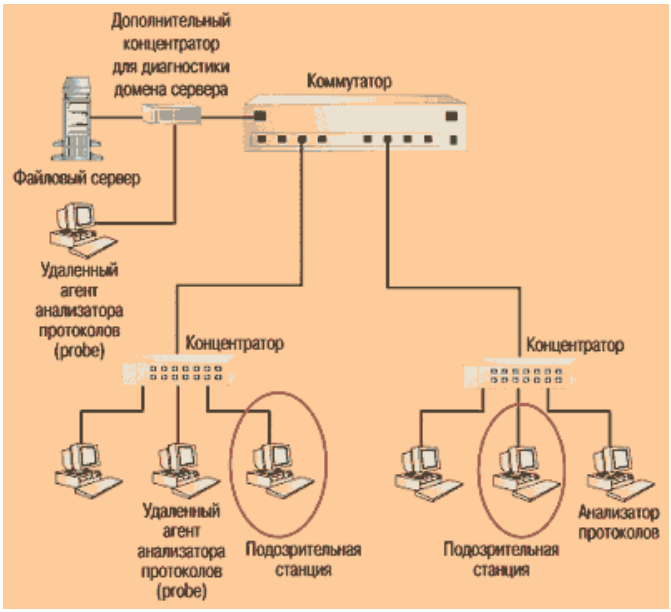


Рисунок - Второй способ подключения анализатора

ЛАБОРАТОРНАЯ РАБОТА №17
ТЕМА: Исследование методов цифровой обработки сигналов на основе сигнальных процессоров в защищенных системах радиосвязи

Шумоподавление для звука

Звуковой сигнал, записываемый в реальных акустических условиях, часто содержит нежелательные шумы, которые могут порождаться окружающей средой или звукозаписывающей аппаратурой. Один из классов шумов - *аддитивные стационарные шумы*.

*Аддитивность*означает, что шум суммируется с "чистым" сигналом и не зависит от него.

Стационарность означает, что свойства шума (мощность, спектральный состав) не меняются во времени.

Примерами таких шумов могут являться постоянное шипение микрофона или усилительной аппаратуры, гул электросети. Работа различных приборов, не меняющих звучания по времени (вентиляторы, компьютеры) также может создавать шумы, близкие к стационарным. Не являются стационарными шумами различные щелчки, удары, шелест ветра, шум автомобилей.

Для подавления аддитивных стационарных шумов существует алгоритм *спектрального вычитания*. Он состоит из следующих стадий:

1. Разложение сигнала с помощью кратковременного преобразования Фурье (STFT) или другого преобразования, компактно локализующего энергию сигнала.
2. Оценка спектра шума.
3. "Вычитание" амплитудного спектра шума из амплитудного спектра сигнала.
4. Обратное преобразование STFT - синтез результирующего сигнала.

В качестве банка фильтров рекомендуется использовать STFT с окном Ханна длиной порядка 50 мс и степенью перекрытия 75%. Амплитуду весового окна надо отмасштабировать так, чтобы при выбранной степени перекрытия окон банк фильтров не менял общую амплитуду сигнала в отсутствие обработки.

Оценка спектра шума может осуществляться как автоматически, путем поиска участков минимальной энергии в каждой частотной полосе, так и вручную, путем анализа спектра на временном сегменте, который пользователь идентифицировал как шум.

Одна из проблем метода спектрального вычитания – т.н. «*музыкальный шум»*. Он появляется вследствие того, что коэффициенты STFT шумовых сигналов статистически случайны, что приводит к их неравномерному подавлению. В результате, очищенный сигнал содержит кратковременные и ограниченные по частоте всплески энергии, которые на слух воспринимаются как "колокольчики" или "льющаяся вода". В некоторых случаях этот эффект даже менее желателен, чем исходный подавляемый шум.

Для подавления этого артефакта можно применять следующие методы:

• Завышение оценки шумового порога (увеличение k). Приводит к подавлению слабых компонент полезного сигнала, звук становится глуше.

• Неполное подавление шума (ограничение снизу константой, отличной от нуля). Часть шума остается в сигнале и отчасти маскирует «музыкальный шум».

• Сглаживание по времени оценок спектра. Приводит к размытию или подавлению транзиентов (резких всплесков в сигнале: ударов, атак музыкальных инструментов).

• Адаптивное сглаживание оценок спектра по времени и частоте. Наиболее качественный, но и трудоемкий метод.

Наиболее распространенный способ подавления «музыкального шума» – использует сглаживание спектра по времени. Для этого к STFT-коэффициентам исходного сигнала применяется рекурсивная фильтрация по времени. Более качественного подавления можно достичь, применяя к спектрограмме адаптивные двумерные алгоритмы фильтрации, такие как билатеральный фильтр или алгоритм нелокального усреднения, используемые в шумоподавлении для изображений.

Передискретизация

Ресамплинг(*передискретизация, resampling*) – это изменение частоты дискретизации цифрового сигнала. Применительно к цифровым изображениям ресамплинг означает изменение размеров изображения. Существует множество различных алгоритмов ресамплинга изображений. Например, для увеличения изображения в 2 раза можно просто продублировать каждую из его строк и каждый из его столбцов (а для уменьшения – выкинуть). Такой метод называется методом ближайшего соседа (*nearestneighbor*). Можно промежуточные столбцы и строки получить линейной интерполяцией значений соседних столбцов и строк. Такой метод называется билинейной интерполяцией (*bilinearinterpolation*). Можно каждую точку нового изображения получить как взвешенную сумму большего числа точек исходного изображения (бикубическая и другие виды интерполяции).

Наиболее качественныйресамплинг получается при использовании алгоритмов, учитывающих необходимость работы не только с временной, но и с частотной областью изображения. Сейчас мы рассмотрим алгоритм ресамплинга, который основан на идее максимального сохранения частотной информации изображения. Алгоритм построен по принципу **интерполяция / фильтрация / прореживание** (*interpolation / filtering / decimation*).

Работу алгоритма будем рассматривать на одномерных сигналах, так как двумерное изображение можно сначала растянуть или сжать по горизонтали (по строкам) а потом – по вертикали (по столбцам). Таким образом, ресамплинг двумерного изображения сводится к ресамплингу одномерного сигнала.

Пусть нам нужно «растянуть» одномерный сигнал от длины n точек до длины m точек, т.е. в nmраз. Для выполнения этой операции необходимо выполнить 3 шага. Первый шаг – интерполяция нулями, увеличивающая длину сигнала в m раз. Нужно умножить все отсчеты исходного сигнала на m, а потом после каждого отсчета сигнала нужно вставить m-1 нулевое значение. При этом спектр сигнала изменяется следующим образом. Та часть спектра, которая изначально содержалась в цифровом сигнале, остается без изменения (именно этого мы добиваемся). Но выше старой половины частоты дискретизации возникают помехи (отраженные копии спектра), от которых необходимо избавиться с помощью фильтрации.

Второй шаг – это отфильтровывание этих помех с помощью НЧ-фильтра. Теперь мы получили сигнал, который в m раз длиннее исходного, но сохранил его частотную информацию и не приобрел посторонней частотной информации (ее мы отфильтровали). Если бы нашей задачей было удлинение сигнала в m раз, то на этом шаге можно было бы остановиться. Но наша задача требует теперь уменьшить длину сигнала в n раз. Для этого нужно выполнить 2 шага. Первый шаг – это антиалиасинговая фильтрация. Так как частота дискретизации уменьшается в n раз, то из спектра сигнала, согласно теореме Котельникова, удастся сохранить только его низкочастотную часть. Все частоты выше половины будущей частоты дискретизации нужно удалить с помощью антиалиасингового фильтра с частотой среза равной n1 от текущей половины частоты дискретизации. Второй шаг – это прореживание полученного сигнала в n раз. Для этого достаточно выбрать из сигнала каждый n-й отсчет, а остальные – отбросить. Этот алгоритм очень схож с работой АЦП, который тоже сначала отфильтровывает ненужные частоты из сигнала, а потом замеряет Заметим, что две НЧ-фильтрации, применяемые в этом алгоритме друг за другом, можно (и нужно) заменить одной. Для этого частоту среза единого НЧ -фильтра нужно выбрать равной минимуму из частот среза двух отдельных НЧ-фильтров. Еще одно существенное улучшение алгоритма – это поиск общих делителей у чисел m и n. Например, очевидно, что для того, чтобы сигнал из 300 точек сжать до 200 точек, достаточно положить в алгоритме m=2 и n=3.

Заметим, что приведенный алгоритм требует очень большого объема вычислений, т.к. промежуточный размер одномерного сигнала при ресамплинге может быть порядка сотен тысяч. Существует способ существенно повысить быстродействие алгоритма и сократить расход памяти. Этот способ называется *многофазной фильтрацией* (*polyphasefiltering*). Он основан на том, что в длинном промежуточном сигнале совсем необязательно вычислять все точки. Ведь большая часть из них все равно будет отброшена при прореживании. Многофазная фильтрация позволяет

непосредственно выразить отсчеты результирующего сигнала через отсчеты исходного сигнала и антиалиасингового фильтра.

Отметим, что здесь мы не рассматриваем такие детали алгоритма, как коррекция границ изображения, выбор фазы сигнала при интерполяции и прореживании и построение хорошего антиалиасингового фильтра. Отметим только, что для ресамплинга изображений требуется уделить особое внимание как частотной, так и пространственной характеристике фильтра. Если оптимизировать фильтр только в частотной области, то это приведет к большим пульсациям в ядре фильтра. А при ресамплинге изображений пульсации в ядре фильтра приводят к пульсациям яркости вблизи резких перепадов яркости в изображении (***эффект Гиббса**, Gibbsphenomenon*)

Антиалиасинг изображений

Избежать алиасинга при генерации изображений – важная задача компьютерной графики. Алиасинг в изображениях приводит к зубчатости краев фигур, муару, плохой читаемости текста и графиков. Одним из основных способов предотвращения алиасинга является так называемый*суперсамплинг*(*super-sampling*). Этот прием заключается в генерации изображения с большим разрешением и ресамплингу этого изображения до нужного размера. Рассмотрим пример. Пусть нам нужно сгенерировать трехмерное изображение шахматной доски с разрешением 200x150 пикселей. Если сделать это непосредственно (например, трассировкой лучей через каждую точку экрана), то результат может быть существенно искажен алиасингом. Применим метод суперсамплинга. Сгенерируем нужное нам изображение с четырехкратным размером 800x600 пикселей, а затем уменьшим его до размера 200x150. Заметим, что качество получаемого таким образом изображения существенно лучше и зависит от качества алгоритма ресамплинга и от степени суперсамплинга (во сколько раз большее изображение мы сгенерировали). Желательно применять алгоритм ресамплинга, обеспечивающий хороший антиалиасинг.

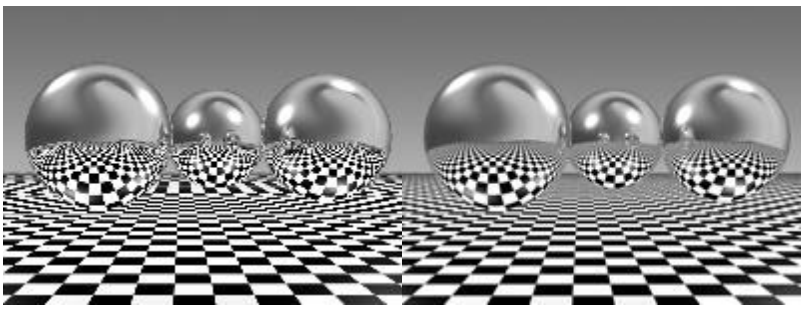


Рисунок. Изображение, сгенерированное без антиалиасигна и с антиалиасингом.

Рассмотренный алгоритм широко применяется в компьютерной графике, несмотря на большие вычислительные затраты. Выбирая степень суперсамплинга, можно варьировать производительность алгоритма. Очевидно, что сложность алгоритма квадратично зависит от степени суперсамплинга. Обычно используются степени суперсамплинга от двух до четырех.

Псевдотонирование изображений

Псевдотонирование(*half-toning*) – это создание иллюзии полноцветности изображения с помощью небольшого реального числа цветов. Пример псевдотонирования – фотографии в газетах, где любые оттенки серого передаются с помощью чередования мелких черных и белых точек.

Мы рассмотрим вариант псевдотонирования для черно-белых изображений. Нашей задачей будет представить изображение с оттенками серого в виде монохромного (двухцветного) изображения.

Пусть мы имеем изображение в оттенках серого, интенсивность точек которого может принимать произвольные значения от 0 до 1. Рассмотрим некоторые алгоритмы приведения такого изображения к монохромному, яркость точек которого может принимать 2 значения: 0 или 1.

Первый самый простой алгоритм – это усечение (порог). Все пиксели с яркостью больше 0.5 получают яркость 1, все остальные – яркость 0. Такой алгоритм обычно дает наихудшие результаты.

Более качественные алгоритмы стремятся так распределить черные и белые пиксели в полученном изображении, чтобы на каждом участке изображения концентрация белых пикселей была пропорциональна яркости этого участка в исходном изображении.

Один из таких методов – *упорядоченноепсевдотонирование*. В этом методе исходное изображение разбивается на небольшие блоки одинакового размера (например, 3x3). Затем в каждом блоке находится средняя яркость изображения. В соответствии с этой средней яркостью выбирается количество белых пикселей в соответствующем блоке получаемого монохромного изображения. Обычно эти белые пиксели упорядочиваются в соответствии с некоторым регулярным шаблоном (рис. 15).

Существуют другие алгоритмы достижения нужной концентрации белых пикселей в получаемом монохромном изображении. Например, существует класс алгоритмов, которые достигают этого в 2 стадии. Сначала к изображению добавляется случайный шум необходимой амплитуды, а затем применяется порог. Такие алгоритмы называют *диттерингом*(***dithering***).

Шум представляет собой некий достаточно случайный сигнал, не зависящий от изображения. Например, белый шум – это просто последовательность случайных чисел с математическим ожиданием 0. Спектр такого шума приблизительно равен константе на всех частотах (в пределах половины частоты дискретизации). Последовательные отсчеты такого шума не коррелируют между собой.

Существуют другие виды шума. Например, у розового шума энергия обратно пропорциональна частоте (в определенном рассматриваемом диапазоне частот). Другими словами, амплитуда его гармоник падает на 3 дБ при удвоении частоты. У голубого шума энергия наоборот растет с частотой. Существуют и другие виды шума, однако определения для них могут быть различны в разных областях.

Будем называть ошибкой квантования изображение, равное разности исходного и псевдотонированного изображений.

При псевдотонировании изображений стремятся добиться того, чтобы спектр изображения-ошибки по возможности не содержал низкочастотных и среднечастотных компонент. В этом случае ошибка будет менее заметна человеческому глазу. Например, при диттеринге розовым шумом спектр ошибки тоже близок к светло-розовому, и результирующее изображение выглядит значительно искаженным (рис. 15). При диттеринге белым шумом спектр ошибки белый. Поэтому результирующее изображение выглядит лучше. При диттеринге с диффузией ошибки спектр ошибки получается близок к голубому шуму, т.е. содержит мало низкочастотных компонент. В результате получается приятное глазу изображение.

Нетрудно видеть, что просто диттеринг голубым шумом не приводит к желаемому результату, т.к. ошибка квантования при этом имеет спектр, содержащий значительное количество низкочастотных и среднечастотных компонент. Для избавления от них нужно применить рекурсивный фильтр. Этот метод псевдотонирования называется ***диффузией ошибки*** (*errordiffusion*). Его идея в том, что ошибка квантования, возникшая при квантовании данного пикселя, распространяется с обратным знаком на соседние пиксели и таким образом как бы компенсируется.

Выравнивание освещенности изображений

Часто некоторые участки на изображении бывают слишком темными, чтобы на них можно было что-то разглядеть.

Если прибавить яркости ко всему изображению, то изначально светлые участки могут оказаться совсем засвеченными. Чтобы улучшить вид изображения в таких случаях, применяется метод выравнивания освещенности.

Этот метод не является линейным, т.е. не реализуется линейной системой. Действительно, рассмотрим модель типичную освещенности для фотографии. Фотографируемый пейзаж обычно

освещен по-разному в разных точках. Причем обычно освещенность меняется в пространстве достаточно медленно.

Мы хотим, чтобы все детали на фотографии были освещены более однородно, но при этом оставались достаточно контрастными друг относительно друга.

А на реальной фотографии получается произведение той картинки, которую мы хотим видеть и карты освещенности. Там где освещенность близка к нулю, все предметы и детали тоже близки к нулю, то есть практически невидимы.

Поскольку освещенность меняется в пространстве достаточно медленно, то можно считать ее низкочастотным сигналом. Само же изображение можно считать в среднем более высокочастотным сигналом. Если бы в процессе фотографии эти сигналы складывались, то их можно было бы разделить с помощью обычного фильтра.

Например, применив ВЧ-фильтр, мы бы «избавились от перепадов освещенности» (НЧ-сигнала), а оставили «само изображение». Но поскольку эти сигналы не складываются, а перемножаются, то избавиться от неравномерностей освещенности простой фильтрацией не удастся.

Для решения таких задач применяется *гомоморфная обработка*. Основной метод гомоморфной обработки заключается в сведении нелинейной задачи к линейной с помощью каких-либо преобразований. Например, в нашем случае можно свести задачу разделения перемноженных сигналов к задаче разделения сложенных сигналов. Для этого нужно взять логарифм от произведения изображений.

Логарифм от произведения равен сумме логарифмов сомножителей. Если учесть, что логарифм от НЧ-сигнала остается НЧ-сигналом, а логарифм от ВЧ-сигнала остается ВЧ-сигналом, то мы свели задачу разделения произведения сигналов к задаче разделения суммы НЧ- и ВЧ-сигналов. Очевидно, эту задачу можно решить с помощью ВЧ-фильтра, который удалит из суммы сигналов низкие частоты. После этого останется только взять от полученного сигнала экспоненту, чтобы вернуть его к исходному масштабу амплитуд.

ВЧ-фильтр можно реализовать следующим образом. Сначала к изображению применяется операция размытия (НЧ-фильтр), а потом из исходного изображения вычитается размытое.

Наилучший радиус размытия зависит от конкретного изображения. Можно начать эксперименты с радиуса порядка десяти пикселей.

Обычно для размытия изображения применяется двумерный гауссовский фильтр.

Непосредственное вычисление двумерной свертки с таким ядром потребует огромных вычислений даже при сравнительно небольшом размере ядра. Однако приведенное гауссово ядро обладает свойством ***сепарабельности***.

Это означает, что эквивалентного эффекта можно достичь, отфильтровав сначала все строки изображения одномерным гауссианом, а затем отфильтровав все столбцы полученного изображения таким же одномерным гауссианом.

Полученный от выравнивания освещенности эффект может оказаться слишком сильным (темные области станут по яркости такими же, как и светлые). Чтобы уменьшить эффект, можно просто смешать обработанное изображение с исходным в определенной пропорции.

Другие применения

Улучшение изображений и художественные эффекты

Для улучшения изображений и создания различных художественных эффектов часто применяется фильтрация. Например, для придания изображению резкости можно воспользоваться фильтром, который усиливает сигнал на высоких частотах. Существуют фильтры для выделения или нахождения границ в изображении, размытия, направленного смазывания изображений, создания различных эффектов, таких как акварель, тиснение.

Поиск фрагментов в изображениях

Для поиска фрагментов в изображениях применяется двумерная корреляция. Сигналом для поиска является изображение, а искомым сигналом – искомый фрагмент изображения. Эффективное вычисление корреляции стало возможным благодаря двумерному БПФ.

Компрессия изображений

Методы цифровой обработки сигналов позволяют достаточно эффективно сжимать изображения в частотной области. Например, алгоритм JPEG действует следующим образом (упрощенно). Изображение разбивается на фрагменты размером 8x8 пикселей, и каждый фрагмент переводится в частотную область. После этого в каждом фрагменте те высокочастотные составляющие, амплитуда которых мала, выкидываются, а все остальные – кодируются. Ясно, что для тех областей изображения, где яркость изменяется, не очень быстро (а таких большинство), высокочастотных компонент почти нет. Таким образом, удается выкинуть из спектра существенную часть не очень важной информации. В JPG-файле кодируются оставшиеся «существенные» амплитуды.

В алгоритме JPEG применяется модификация ДПФ: дискретное косинусное преобразование (ДКП). ДКП от двумерного сигнала можно вычислить, отразив четным образом сигнал относительно нулевой точки и вычислив двумерное ДПФ полученного сигнала с двукратными размерами. В полученном спектре будут содержаться только «косинусные» коэффициенты.

Восстановление изображений

При съемке движущегося объекта неподвижной камерой полученное изображение получается смазанным. Если знать параметры движения объекта, то можно построить ядро свертки, которое камера «применила» к снимаемому сигналу. Затем с помощью метода деконволюции можно в значительной степени устранить эффект размытия.

Иногда при съемке камера может вносить в изображение интерференцию – периодический муар, накладываемый на изображение. Часто оказывается, что спектр этой интерференции состоит из одной – двух гармоник. В этом случае ее можно эффективно удалить с помощью фильтра, который подавляет заданные частоты (*notchfilter*).

ЛАБОРАТОРНАЯ РАБОТА №18
ТЕМА: Установка и настройка оборудования по защите информации

Задание: рассмотреть комплексную систему защиты информационных ресурсов объекта.

Объект защиты представляет собой кабинет, расположенный на втором этаже трех этажного здания, с двух сторон окруженный помещениями организации. Третья сторона выходит в коридор, а четвертая стена является внешней здания и выходит на территорию контролируемой зоны.

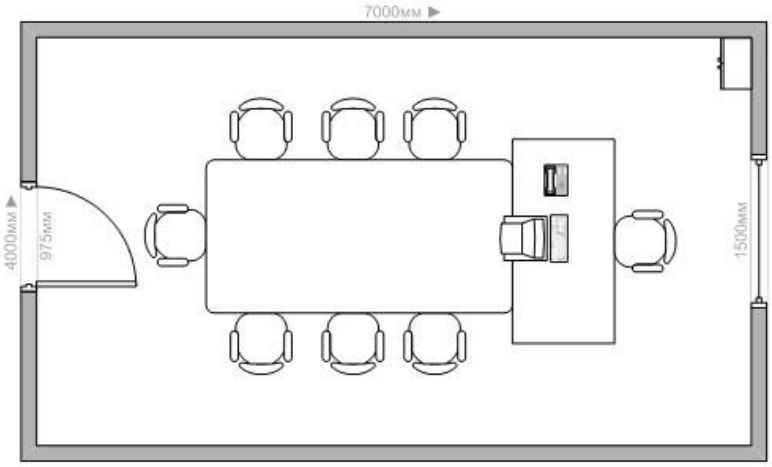


Рис 1. Схематический план объекта защиты

Контролируемая зона – это территория объекта, на которой исключено неконтролируемое пребывания лиц не имеющие постоянного или разового доступа.

Для данного объекта необходимы средства защиты информации от утечки по каналам утечки:

- визуально-оптическому каналу;
- виброакукстическому каналу;
- ПЭМИН;
- утечка по телефонной линии;
- утечка по телекоммуникационным сетям;
- НСД.

Для решения поставленной защиты объекта предлагаются следующие технические решения.

Телефонный скремблер «Грот»

Предназначен для шифрования речевого сигнала и защиты факсимильных сообщений, передаваемых по телефонной сети общего применения.

Работа в канале:

- напряжение постоянного тока в абонентской линии: от 30 до 60 В;
- высокая помехоустойчивость при работе в канале связи;
- автоматическая адаптация к телефонному аппарату абонента, абонентской линии, нелинейности трактов АТС;
- устойчивость работы в реальных телефонных каналах России и стран СНГ, включая междугородные и международные с радиорелейными вставками и любыми видами уплотнения;
- совместимость с любым типом телефонного и факсимильного аппарата, с мини-АТС любого типа, имеющей аналоговый выход;

• работа в линиях, оборудованных системами уплотнения и используемых для охранной сигнализации;

Пользовательские свойства:

• высокая степень эхокомпенсации;
• низкий уровень шумов в телефонной трубке;
• высокое качество восстановленной речи;
• речевая поддержка режимов работы;
• энергонезависимая память индивидуальных ключей-идентификаторов;
• упрощенный алгоритм ввода индивидуальных ключей-идентификаторов за счет использования электронного блокнота индивидуальных ключей;

Шифрование:

• метод шифрования – мозаичный: частотные и временные перестановки;
• метод открытого распределения ключей, позволяющий работать без ручного набора ключей;
• общее количество ключевых комбинаций 2*1018;
• возможность введения дополнительного 7-ми значного ключа для идентификации абонента;
• высокая степень криптографической защиты за счет наличия дополнительных мастер-ключей, которые устанавливаются по желанию Заказчика;

Технические характеристики:

• потребляемая мощность не более 2,5 Вт;
• питание от сетевого адаптера или внешних батарей9-12 В;
• габариты 115х200х30 мм; вес: не более 0,8 кг.

Электрические параметры по стыку с телефонной линией:

• напряжение постоянного тока в абонентской линии от 30 до 60 В;
• модуль входного электрического сопротивления в разговорном режиме в режиме закрытой связи в диапазоне частот от 300 Гц до 3,4 кГц от 500 до 750 Ом;
• модуль входного электрического сопротивления в режиме ожидания вызова в диапазоне частот от 300 Гц до 3,4 кГц от 12 до 15 кОм;
• напряжение постоянного тока на разъеме ЛИНИЯ в режиме закрытой связи при токе в линии от 20 до 25 мА от 6 до 13 В;
• диапазон частот по уровню 3 дБ в режиме закрытой связи от 300 Гц до 2,7 кГц.

Система постановки виброакустических и акустических помех «Шорох-1М»

Система Шорох-1М предназначена для обеспечения защиты выделенных помещений любых категорий от утечки речевой информации по каналам акустики и вибраций.

Выполнение основных требований, предъявляемых к системам защиты от утечки информации:

• сертификация по требованиям ФСТЭК России;
• встроенные системы контроля работоспособности системы;
• наличие дистанционного управления;
• отсутствие каналов утечки за счёт акустоэлектрических преобразований в элементах системы.

Особенности системы:

- расширенный диапазон частот (от 100 Гц до 12 кГц);
- возможность подключения вибровозбудителей разных типов (высокоомных пьезоэлектрических типа КВП и низкоомных электродинамических типа ПЭД);
- расширенные возможности системы контроля функционирования;
- возможность размещения в выделенных помещениях любой категории;
- дистанционное управление и «акустопуск»;
- неограниченная возможность наращивания системы;
- независимые регулировки отдельных каналов.

Сетевой фильтр «ФСПК-100»

Предназначен для предотвращения утечки информации по цепям электропитания, а также для защиты средств оргтехники от внешних помех.

Генератор шума «ГШ-1000У»

Предназначен для маскировки побочных информативных электромагнитных излучений и наводок персональных компьютеров, компьютерных сетей и комплексов на объектах вычислительной техники 1, 2 и 3 категорий в диапазоне частот 0,1-1800 МГц путем формирования и излучения в окружающее пространство маскирующего электромагнитного поля шума (ЭМПШ). Дополнительно имеет 4 независимых коаксиальных выхода некоррелированного напряжения шума, к которым можно подключать:

- устройства ввода маскирующего напряжения шума (например, ответвитель "Дух ") в сети электропитания, заземления, инженерные коммуникации и т.д.;
- дополнительные выносные антенны.

В состав генератора шума входит пять независимых генераторов шума, один из которых нагружен на антенну в виде кольца, а четыре имеют коаксиальные выходы СР-50-73 ФВ для подключения внешних устройств. Независимые генераторы шума могут включаться в любом сочетании по условиям конкретного объекта информатизации. На каждом из четырех коаксиальных 50 Ом выходах генератора шума сформирован широкополосный шумовой сигнал высокой спектральной плотности напряжения. К этим выходам могут быть подключены внешние устройства: дополнительные антенны для улучшения пространственных и поляризационных характеристик излучаемого ЭМПШ, внешние токосъемники, ответвители для ввода напряжения шума в сети питания, заземления, ВТСС, инженерные коммуникации для маскировки информативных наводок создаваемых средствами вычислительной техники. Спектральная плотность напряжения сигнала шума достаточна для обеспечения защиты обрабатываемой средствами вычислительной техники информации от несанкционированного доступа при использовании различных внешних устройств. При использовании в качестве внешних устройств

ответвителей "Дух" для ввода напряжения шума в сети питания, заземления, ВТСС, инженерные коммуникации, которые могут входить в комплект поставки генератора по желанию Заказчика, их можно размещать в удаленных точках защищаемого помещения, соединяя с генератором радиочастотным кабелем. Возможная длина кабеля зависит от вносимых им потерь и, как правило, не для дешевого общеупотребительного кабеля, не менее 10 м.

Электронный замок - комплекс СЗИ НСД «Аккорд-АМДЗ»

Представляют собой аппаратный контроллер, предназначенный для установки в слот ISA (модификация 4.5) или PCI (модификация 5.0). Модули «Аккорд-АМДЗ» обеспечивают доверенную загрузку операционных систем любого типа с файловой структурой FAT12, FAT16, FAT32, NTFS, HPFS, Free BSD, Linux EXT2FS.

Вся программная часть модулей (включая средства администрирования), журнал событий и список пользователей размещены в энергонезависимой памяти контроллера. Таким образом, функции идентификации/аутентификации пользователей, контроля целостности аппаратной и программной среды, администрирования и аудита выполняются самим контроллером до загрузки ОС.

Основные возможности:

- идентификация и аутентификация пользователя с использованием ТМ-идентификатора и пароля длиной до 12 символов;
- блокировка загрузки ПЭВМ с внешних носителей;
- ограничение времени работы пользователей;
- контроль целостности файлов, аппаратуры и реестров;
- регистрация входа пользователей в систему в журнале регистрации;
- администрирование системы защиты (регистрация пользователей, контроль целостности программной и аппаратной части ПЭВМ).

Дополнительные возможности:

- контроль и блокировка физических линий;
- интерфейс RS-232 для применения пластиковых карт в качестве идентификатора;
- аппаратный датчик случайных чисел для криптографических применений;
- дополнительное устройство энергонезависимого аудита.

ЛАБОРАТОРНАЯ РАБОТА №19

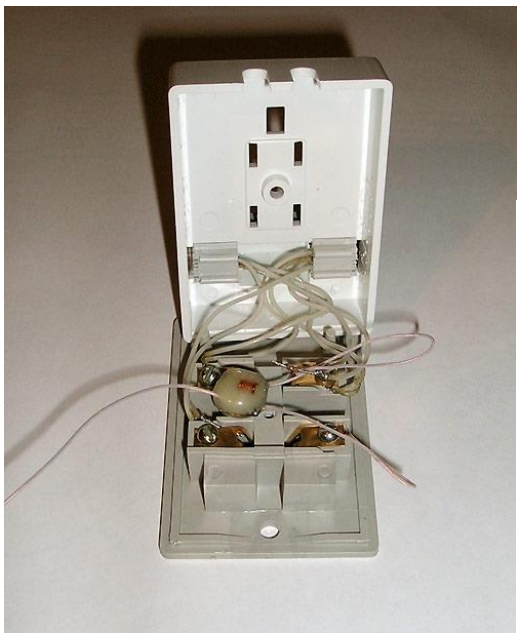
ТЕМА: Обнаружение «радио-жучков»

Поиск жучков с помощью специальных технических средств предполагает привлечение сотрудников организаций, специализирующихся на этом, и выполнение работы специалистами. И чтобы понимать, насколько сложна эта работа с точки зрения обычного человека и неспециалиста, кратко рассмотрим основные технические средства, применяемые для поиска жучков, а потом ознакомимся с условиями для успешного поиска жучков с помощью специальных технических средств.

Самые простые и распространённые средства поиска – это**детекторы поля** и **поисковые широкополосные и сканирующие приемники с захватом частоты**. Такие устройства позволяют выявить наличие радио сигнала и определить место излучения по максимальному уровню излучаемого сигнала. Сканирующий приемник ищет наличие излучения в нескольких определённых диапазонах.

Поиск жучков металлодетектором.Жучок – электронное устройство, поэтому содержит как металлические, так и неметаллические компоненты. А металлодетектор - это устройство, которое применяется в тех случаях, когда необходимо проверить предметы на наличие металлов, но заглянуть внутрь предметов без их разборки нет возможности. Классический пример – рамка на входе в ж.д. вокзал или аэропорт. Для поиска жучков используют портативныеметаллодетекторы.

Поиска жучков нелинейным локатором. Работа такого устройства основана на том, что этот прибор обнаруживает полупроводниковые элементы (диоды, транзисторы, микросхемы и др.), которые обязательно есть во всех жучках. Этот прибор хорош тем, что при умелом использовании может обнаружить и неработающие жуки, которые включаются дистанционно или по заданному времени.



Поиск жучков на линиях телефонной связи, Интернета и других проводных коммуникациях состоит в том, чтобы измерить их электротехнические параметры и сравнить с исходными. Если разница отличается, то можно предполагать о наличии в линии жучка. На картинке показан жучок в телефонной розетке.

Поиск скрыто установленных видео камер осуществляется приборами с подсветкой.Поскольку любая видео камера имеет стеклянный объектив, то работа такого прибора основана на нахождении блика от объектива видео камеры. Прибор излучает световой поток красного цвета, и отражённый блик от линзы скрытой камеры, наблюдаемый через прибор, виден в виде красной точки. Блик не изменяет интенсивность своего свечения до тех пор, пока прибор находится поле обзора камеры.

Использование выше рассмотренных технических средств не является 100% гарантом обнаружения жучков, но в большинстве случаев их достаточно для поиска скрыто установленных электронных устройств.

Процесс поиска техническими средствами включает в себя выполнения предварительных организационных мероприятий, с последующим соблюдением некоторых условий. Если это конспиративный поиск, то речь идёт о том, что «противник не дремлет», и он не должен знать о том, что будут выполнены работы по поиску жучков. А в процессе поиска (если жучок работает) противник не должен подозревать о том, что идёт поиск. И по окончанию поисковых работ необходимо выполнить демаскирующие мероприятия. Несоблюдение конфиденциальности в значительной степени затруднит поиск. Если поиск жучков это плановое мероприятие, то его выполняют периодически, на конкретных объектах, и как правило с привлечением специалистов сторонних организаций.

В зависимости от предполагаемого типа жучка (на линии связи, на электрической линии, радиоканал, видео и т.д.), применяют определённые устройства и конкретную методику поиска, направленные именно на этот тип.

ЛАБОРАТОРНАЯ РАБОТА №20
ТЕМА: Изучение принципа работы детектора поля.

1. Назначение и принцип действия детектора поля.
2. Основные характеристики детектора поля.
3. Принцип действия акустической завязки.
4. Порядок поиска подслушивающих устройств.
5. Порядок поиска при высоком уровне помех.

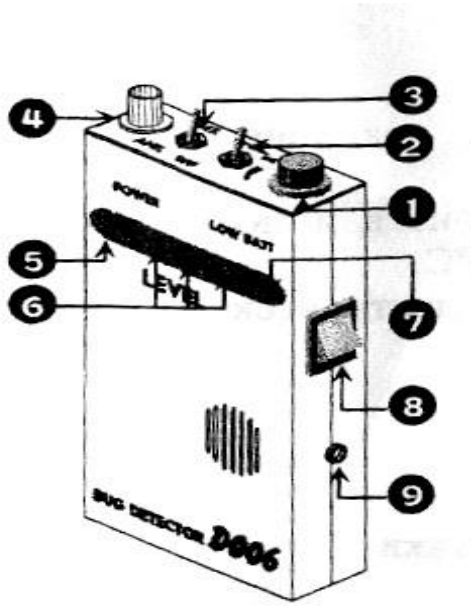
Детектор поля D 006.

Детектор D 006 предназначен для оперативного обнаружения радиопередающих прослушивающих систем промышленного шпионажа (РС).

Данный прибор является конечным элементом поиска подобных устройств и позволяет в конкретной обстановке выявить и локализовать скрытно установленные РС.Принцип действия **D 006** основан на широкополосном детектировании электрического поля, что дает возможность регистрировать РС независимо от вида модуляции.

Технические характеристики детектора D 006:

Характеристика	**Значение**
Питание	9В
Потребляемый ток	30 Ма
Габариты D 006	128×63×20(мм)
Диапазон частот	50÷1000(МГц)
Чувствительность (f=110МГц)	0,5мВ
Чувствительность (f=800МГц)	3мВ
Динамический диапазон индикатора	40дБ



1. Выключатель питания и регулятор порога срабатывания
2. Выключатель тонального звукового сигнала
3. Выключатель аттенюатора
4. Разъем для подключения антенны
5. Индикатор включения питания
6. Индикатор уровня электрического поля

7. Индикатор разряда аккумулятора
8. Выключатель системы акустической обратной связи
9. Разъем для подключения зарядного устройства

Радиус обнаружения детектора зависит от излучаемой мощности прослушивающей системы, электромагнитной обстановки в обследуемом помещении и составляет при мощности РС 5мВт порядка 1м.

Возможность включение аттенюатора облегчает работу в условиях сложной электромагнитной обстановки, присущей крупным промышленным центрам, за счет ослабления входного сигнала. Данный режим полезен и в случае точного обнаружения мощных РС.

Наличие системы акустической обратной связи («акустической завязки») позволяет исключить ложные срабатывания детектора на локальные электромагнитные поля и идентифицировать находящееся в помещении РС по характерному звуковому сигналу.

Восьмисегментная логарифмическая светодиодная шкала и тональный звуковой сигнал обеспечивают наглядность и удобство при работе с прибором.

Порядок работы:

1. Установите регулятором (1) положение max чувствительности. Для этого, находясь на относительном удалении от предполагаемых мест установки РС (например, в свободном от мебели центре комнаты), поворачивайте ручку регулятора вправо до начала загорания второго сегмента шкалы индикатора (6) (выключатель (3) при этом должен находиться в положении «OFF»).

2. В случае, если при максимальном загрубении чувствительности детектора (регулятор (1) повернут против часовой стрелки до упора) на индикаторе (6) горит более двух сегментов, что говорит о высоком уровне электромагнитных полей на объекте, включите аттенюатор (выключатель (3) в положении «АТТ»). Это позволит Вам работать в данных условиях при соответствующем уменьшении максимальной дальности обнаружения примерно в 2–3 раза.

3. В процессе работы с прибором могут создавать помехи побочные излучения бытовых электроприборов, телевизоры, компьютеры, различные наводки от проводов сети 220В×50Гц. Предварительно изучите характер их действия и особенности распространения.

4. При осмотре объекта проводите антенной прибора вдоль предполагаемых мест установки РС. Увеличение количества одновременно горящих светодиодов индикатора (6) и усиление тона звукового сигнала позволят Вам точно установить их месторасположение.

5. Для уменьшения чувствительности и соответственно повышения точности локализации РС плавно поворачивайте регулятор (1) против часовой стрелки.

Для однозначной идентификации включите акустическую завязку (систему акустической обратной связи) (выключатель (8) в положении «AUD»). На нахождение РС в зоне обнаружения детектора однозначно укажет характерный звуковой тон. В противном случае будет прослушиваться хаотичный шум.

6. Для более точного определения меняйте ориентацию антенны.

Дополнительные рекомендации:

1. Некоторые типы РС включают свои радиопередающие блоки только в случае наличия какого-либо звукового шума в помещении. Поэтому перед проведением осмотра включите один из стандартных источников звука: например радиоприемник.

2. Во избежание отключения на время проверки дистанционно управляемых систем не ведите предварительных и сопутствующих разговоров во время осмотра помещения, дающих представление о Вашей деятельности.

3. Детектор эффективен при обнаружении телефонных РС. В качестве передающей антенны используется в основном телефонный провод. Для обнаружения таких устройств проведите следующие действия:

3.1. замерьте уровень излучения в непосредственной близости от телефонного провода при опущенной телефонной трубке;

3.2. поднимите трубку и повторите измерения; увеличение сигнала укажет на наличие подключенной к линии РС.

4. Для зарядки аккумулятора проведите следующие действия:

1.1. подключите в разъем (9) ответную часть зарядного устройства, предварительно выключив детектор;

1.2. подключите зарядное устройство к сети 220В; время полной зарядки составляет 14 часов.

Во избежание выхода из строя детектора ***запрещается*** *использование* ***D 006*** *в непосредственной близости от радиопередающих устройств мощностью более 1 Вт.*

ЛАБОРАТОРНАЯ РАБОТА №21

ТЕМА: Установка и настройка программных средств защиты информации.

ЦЕЛЬ: ИЗУЧИТЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Система криптографической защиты информации от НСД КРИПТОН-ВЕТО предназначена для защиты персонального компьютера, который при этом может использоваться в качестве: • абонентского пункта; • центра коммутации пакетов; • центра выработки ключей.

Система ограничивает круг лиц и их права доступа к информации на персональном компьютере. Ее реализация основана на технологиях "прозрачного" шифрования логических дисков и электронной цифровой подписи

В состав основных функций системы КРИПТОН-ВЕТО включены следующие:

• обеспечение секретности информации в случае кражи "винчестера" или ПК;

• обеспечение защиты от несанкционированного включения компьютера;

• разграничение полномочий пользователей по доступу к ресурсам компьютера;

• проверка целостности используемых программных средств системы в момент включения системы;

• проверка целостности программы в момент ее запуска на выполнение;

• запрещение запуска на выполнение посторонних программ;

• ведение системного журнала, регистрирующего события, возникающие в системе;

• обеспечение "прозрачного" шифрования информации при обращении к защищенному диску;

• обнаружение искажений, вызванных вирусами, ошибками пользователей, техническими сбоями или действиями злоумышленника.

Основным аппаратным элементом системы являются серийно выпускаемые аттестованные ФАПСИ платы серии КРИПТОН, с помощью которых проверяется целостность системы и выполняется шифрование. Система предполагает наличие администратора безопасности, который определяет взаимодействие между управляемыми ресурсами: • пользователями; • программами; • логическими дисками; • файлами (дискреционный и мандатный доступ); • принтером; • дисководами.

Система обеспечивает защиту следующим образом. Жесткий диск разбивается на логические диски. Первый логический диск (С:) отводится для размещения системных программ и данных; последний логический диск - для размещения СЗИ НСД и доступен только администратору. Остальные логические диски предназначены для хранения информации и программ пользователей. Эти диски можно разделить по пользователям и/или по уровню секретности размещаемой на них информации.

Можно выделить отдельные диски с информацией различного уровня секретности (доступ к таким дискам осуществляется с помощью специальной программы, проверяющей допуск пользователя к документам-файлам). Сначала администратор устанавливает уровень секретности диска, а затем определяет круг лиц, имеющих доступ к этому диску.

По форме хранения информации диски подразделяются на открытые и шифруемые; по уровню доступа - на доступные для чтения и записи, доступные только для чтения, недоступные

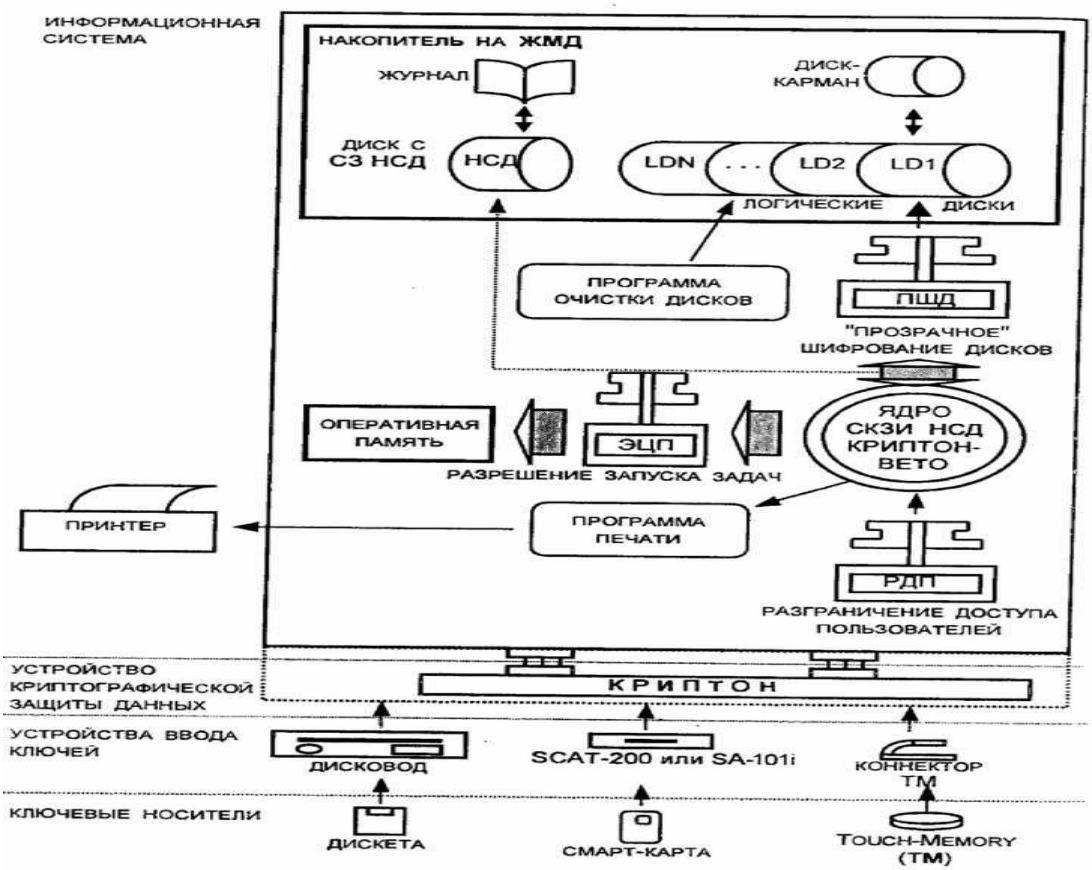
(заблокированные). Недоступный диск делается невидимым в DOS и, следовательно, не провоцирует пользователя на несанкционированный доступ к нему. Доступный только для чтения диск можно использовать для защиты не только от целенаправленного, но также от непреднамеренного (случайного) искажения (удаления) информации. Открытый диск ничем не отличается от обычного логического диска DOS. Очевидно, что системный диск должен быть открыт.

Для шифруемых дисков используется шифрование информации в прозрачном режиме. При записи информации на диск она автоматически шифруется, при чтении с диска автоматически расшифровывается. Каждый шифруемый диск имеет для этого соответствующий ключ. Последнее делает бесполезными попытки улучшения своих полномочий пользователями, допущенными на ПК, поскольку они не имеют ключей доступа к закрытым для них дискам. Наличие шифрования обеспечивает секретность информации даже в случае кражи жесткого диска.

Для допуска к работе на ПК администратором формируется список пользователей, в котором:

- указывается идентификатор и пароль пользователя;
- определяется уровень допуска к секретной информации;
- определяются права доступа к логическим дискам.

В дальнейшем только администратор может изменить список пользователей и их полномочия. Для исключения возможности установки на ПК посторонних программ с целью взлома защиты администратор определяет перечень программ, разрешенных к запуску на данном компьютере. Разрешенные программы подписываются администратором электронно-цифровой подписью (ЭЦП). Только эти программы могут быть запущены в системе. Использование ЭЦП одновременно с наличием разрешения позволяет отслеживать целостность запускаемых программ. Последнее исключает возможность запуска измененной программы, в том числе и произошедшего в результате непредвиденного воздействия "вируса".



Для входа в компьютер используются ключи, записанные на ключевой дискете, смарт-карте или на устройстве Touch-Memory. Ключи изготавливаются администратором системы и раздаются

пользователям под расписку. Для исключения загрузки компьютера в обход СЗ НСД загрузка осуществляется только с жесткого диска. При включении ПК (до загрузки операционной системы) с "винчестера" аппаратно проверяется целостность ядра системы безопасности КРИПТОН-ВЕТО, системных областей "винчестера", таблицы полномочий пользователей. Затем управление передается проверенному ядру системы безопасности, которая проверяет целостность операционной системы. Расшифрование полномочий пользователя, ключей зашифрованных дисков и дальнейшая загрузка операционной системы производятся лишь после заключения о ее целостности. В процессе работы в ПК загружены ключи только тех дисков, к которым пользователю разрешен доступ.

Для протоколирования процесса работы ведется журнал. В нем регистрируются следующие события: • установка системы КРИПТОН-ВЕТО; • вход пользователя в систему (имя, дата, время); • попытка доступа к запрещенному диску (дата, время, диск); • зашифрование диска; • расшифрование диска; • перешифрование диска; добавление нового пользователя;• смена полномочий пользователя;• удаление пользователя из списка;• сброс причины останова системы; • попытка запуска запрещенной задачи;• нарушение целостности разрешенной задачи и т.д.

Журнал может просматриваться только администратором. Для проверки работоспособности системы используются программы тестирования. При необходимости пользователь может закрыть информацию на своем диске и от администратора, зашифровав последнюю средствами абонентского шифрования.

ЛАБОРАТОРНАЯ РАБОТА №22-23
ТЕМА: Система условного доступа Conax

Система условного доступа (CAS) для цифрового видеовещания**Conax CAS7.**

Стандартная сеть платного телевидения - это основной и наиболее стабильный источник дохода для большинства компаний-операторов. Однако отсутствие эффективных каналов заказа программ ограничивает возможности предоставления дополнительных услуг, таких как "Видео по запросу" (VOD), "Почти видео по запросу" (NVOD) и других интересных услуг в области цифрового телевидения.

Операторы мобильной телефонной связи с большим успехом продают карты предварительной оплаты звонков. Большинство абонентов цифрового телевидения имеют также и сотовые телефоны и знакомы с тем, как пользоваться текстовыми сообщениями. Система Conax CAS7 предоставляет возможность заказа услуг цифрового телевидения путём отправки текстового сообщения с сотового телефона. Это позволяет простыми и надёжными методами производить оплату услуг. Оплата может быть произведена со счёта абонента или с помощью кредитной карточки, либо по обычному счёту за услуги цифрового ТВ или за услуги мобильной связи.

Компоненты ядра системы Conax CAS7

Conax CAS7 включает в себя следующие, необходимые для стандартного платного ТВ, обязательные компоненты:

- Сервер SAS (система авторизации абонентов): управляет генерацией сообщений авторизации (EMM) и следит за состоянием всех пользовательских смарт-карт.
- EMM-инжектор: получает EMM-сообщения от сервера SAS, управляет очередями отправки EMM-сообщений и загружает эти сообщения в мультиплексор.
- ECM-генератор: управляет процессами шифрования и упаковки данных о критерии доступа и кодовых слов для услуг с условным доступом.
- Аппаратной модуль защиты: специальный аппаратный модуль для хранения защищённых данных и управления ключами.
- Смарт-карта пользователя: выполняет расшифровку и интерпретацию EMM и ECM, чтобы определить, предоставлять ли пользователю доступ к контенту или нет.

Расширяемость системы

Система Conax CAS7 и её предшественники спроектированы таким образом, что компания-оператор может начать с установки базовой системы поддержки платного ТВ, а затем расширять её дополнительными компонентами, поддерживающими более сложные функции и бизнес-модели.

Conax CAS7 легко обновляется, её можно довести до любого уровня производительности и сделать полностью дублированной по мере роста бизнеса и приобретения дополнительного оборудования.

Архитектура системы CAS предусматривает возможности маршрутизации и удалённого управления системным оборудованием. Одна установка Conax CAS7 способна обслуживать множество компаний-операторов, осуществляя доставку контента через спутник, по кабелю или по наземным каналам цифрового телевидения.

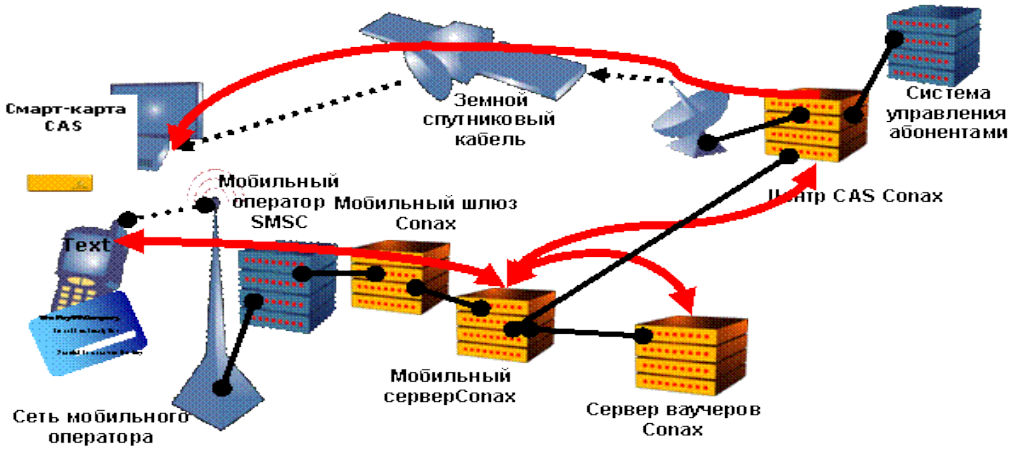
Дополнительные компоненты Conax CAS7

К системе могут быть добавлены различные дополнительных компоненты, расширяющие набор услуг цифрового телевидения:

- Conax CAS7 MobileServer – заказов сервисов по сотовому телефону с помощью SMS-сообщений.

- Conax CAS7 VoucherServer - предоплата услуг при помощи специальных ваучеров (карт предоплаты).
- Conax CAS7 CreditCardServer - оплата услуг с помощью кредитных карточек.
- Conax CAS7 Virtual VOD - приобретение и немедленный просмотр хранимого локально PPV-контента или фильмов с жёсткого диска STB абонента.
- Conax CAS7 Event Pay-Per-View (PPV) - предоставление PPV-услуг.
- Conax CAS7 NVOD – предоставления услуг виртуального кинозала NVOD.
- Conax CAS7 VOD - предоставление услуг "Видео по запросу".
- Conax CAS7 Tokens PPV - поддержка PPV-жетонов.
- Conax CAS7 Messaging - отправка текстовых сообщений конечным пользователям STB-приставок.
- Conax CAS7 EPG/SI Manager - управление воспроизведением событий из таблицы событий (EIT).
- Conax CAS7 DataPlayoutManager - управление любыми данными и их воспроизведением STB-приставками.
- Conax CAS7 Interactive - защита информации при интерактивном взаимодействии, например в on-line тотализаторе.
- Conax CAS7 BMS - управление абонентами, пользовательскими смарт-картами и STB-приставками.
- Conax CAS7 Verifier - дополнительная защита от махинаций и пиратства.
- Conax CAS7 Fingerprinting – используется для отслеживания незаконно распространяемых копий контента.
- Conax CAS7 PVR - защита контента сервиса - виртуальный видеомагнитофон.
- Conax CAS7 ConditionalAccessModule (CAM) – применяется для STB-приставок, поддерживающих общий интерфейс (CI).
- Conax CAS7 OpenCard - используется с STB-приставками, поддерживающими стандарт OpenCable™.
- Conax CAS7 OperationsTools - управления и контроль системой.

Система Conax



Технологии Conax дают возможность телезрителям заказывать DTV-контент, такой как дополнительные ТВ каналы, пакеты каналов, различные спортивные мероприятия, фильмы и игры, посылая текстовые сообщения по сотовому телефону. Доступ к контенту можно продавать, например, на месяц или на неделю, на Новый Год или 8 Марта и т.п. Все это увеличивает доход с одного абонента (ARPU) и сокращает отток пользователей к конкурентам.

Conax предоставляет оператору различные способы оплаты контента.

Существует несколько основных способов оплаты контента DTV: Рассылка счетов абонентам в конце каждого месяца; предоплата за будущие услуги через торговых посредников, используя ваучеры (карты предоплаты); оплата услуг посредством кредитных карт.

Системы Conax поддерживают все эти варианты, а также их комбинации. Например, дополнительный контент может оплачиваться с помощью кредитных карточек, в то время как основные услуги оплачиваются по ежемесячному счёту.

Интерфейс с операторами мобильной связи

Компания Conax разработала универсальный интерфейс с операторами мобильной связи, который значительно облегчает интеграцию с любым таким оператором не зависимо от его географического местоположения.

Принципы реализации сервиса

1) Добавление стоимости контента к счёту за услуги DTV

- Предположим, что доступ к пакету "Развлекательные программы" в выходные дни предлагается за 10 евро.
- Телезритель видит код заказа "РПВД", скажем, на информационном канале.
- Телезритель вносит код "РПВД" в текстовое сообщение и отправляет это сообщение DTV-оператору.
- Если телезритель делает заказ таким способом впервые, он получит текстовое сообщение, в котором его просят послать номер своей смарт-карты условного доступа. Эта информация сохраняется в системе Conax для того, чтобы упростить процедуру дальнейших заказов.
- Телезритель получит подтверждение на свой сотовый телефон и доступ к контенту.
- Стоимость контента добавляется к ежемесячному счёту за услуги DTV.

2) Заказ при помощи ваучера (карты предоплаты)

- Предположим, что пакет "Развлекательные программы" предлагается в качестве месячной подписки.
- Телезритель покупает карту предоплаты в магазине.
- Телезритель вскрывает запечатанный номер на карте, который представляет собой комбинацию кода продукта и "одноразового пароля".
- Номер с карты по сотовому телефону отправляется оператору DTV в соответствии с инструкцией на карте.
- Телезритель принимает на свой сотовый телефон подтверждение от оператора DTV в виде текстового сообщения и получает доступ к контенту.

3) Заказ контента с оплатой кредитной карточкой

- Предположим, что доступ к пакету "Развлекательные программы" в выходные дни предлагается за 10 евро.
- Телезритель видит код заказа "РПВД", скажем, на информационном канале.
- Телезритель вносит код "РПВД" в текстовое сообщение. Затем он добавляет к тому же сообщению три последние цифры из сектора подписи на обратной стороне его кредитной карточки и отправляет сообщение оператору DTV.
- Если телезритель делает заказ таким способом впервые, он получит текстовое сообщение, в котором его просят послать номер своей смарт-карты условного доступа и данные кредитной карточки. Эта информация сохраняется в системе Conax для того, чтобы упростить процедуру дальнейших заказов.
- Телезритель получит подтверждение на свой сотовый телефон и получит доступ к контенту.
- Стоимость контента вычитается из суммы на кредитной карточке.

Conax в IP-телевидении

Отдельные компании-операторы могут распространять контент также и по IP-каналам, таким как xDSL, FTTH и доставлять его на мобильные устройства (DVB-H). Система Conax CAS7 легкго дополняется IP-компонентами ConaxCAstream, выполняющими функции условного доступа как для DVB так и для IP.

Conax CAS7 совместима с открытыми стандартами, такими как MPEG-2, DVB Simulcrypt, OpenCable™, OpenCAS, Docsis и DVB CommonInterface.

Conax CAS7 совместима с STB и мультиплексорами всевозможных вендоров и на разных платформах промежуточного слоя (middleware), включая DVB-MHP, а также SMS-платформы.

Использование широкополосных IP-сетей в качестве канала передачи информации открывает новые возможности для компаний-операторов в виде предоставления дополнительных услуг, используя ту же самую сетевую инфраструктуру. Примерами таких услуг является телефония, широкополосный высокоскоростной доступ, видео по запросу (VOD) и многое др. Эти новые

услуги приведут к повышению показателя ARPU (доход с одного абонента) и сокращению оттока абонентов к конкурентам.

Компания Conax уже обслуживает нескольких клиентов, работающих в области IP-телевидения (IPTV). Основной продукт компании – система Conax CAS7 – разработан для поддержки телевещания по протоколам OAM и IP. Новая технология EdgeOAM, разработанная и поставляемая известными производителями оборудования "head-end", предназначена для поддержки систем, где контент передается несколькими различными методами. Такое новое оборудование имеет выходные сигналы как для OAM, так и IP, что означает, что защита IP-сигналов может быть обеспечена таким же методом, как это делается для сигналов DVB. Таким образом, одна и та же система условного доступа (CA) может работать с обоими видами сигналов.

Например, оператору кабельного телевидения, планирующему оказывать услуги в области IPTV, будет достаточно лишь расширить имеющееся оборудование «головной станции» (head-end) для получения возможности поддержки новых сигналов. Таким образом, все устройства условного доступа, включая смарт-карты, могут продолжать работу также и по протоколу IP. Основные инвестиции оператора пойдут на телеприставки STB и IP-интерфейсы (front-end).

В спектр продукции компании Conax входит также бескарточная система IPTV. В настоящее время эта система находится в стадии разработки, где срок выпуска готового продукта будет зависеть от запросов рынка. Бескарточная система будет базироваться на системе микросхемной защиты телеприставки STB. Компания Conax уже сотрудничает в этой области с несколькими производителями микросхем. Conax не намерен выпускать бескарточную систему на рынок до того, как будет достигнут достаточный уровень защиты микросхем.

ЛАБОРАТОРНАЯ РАБОТА №24-26

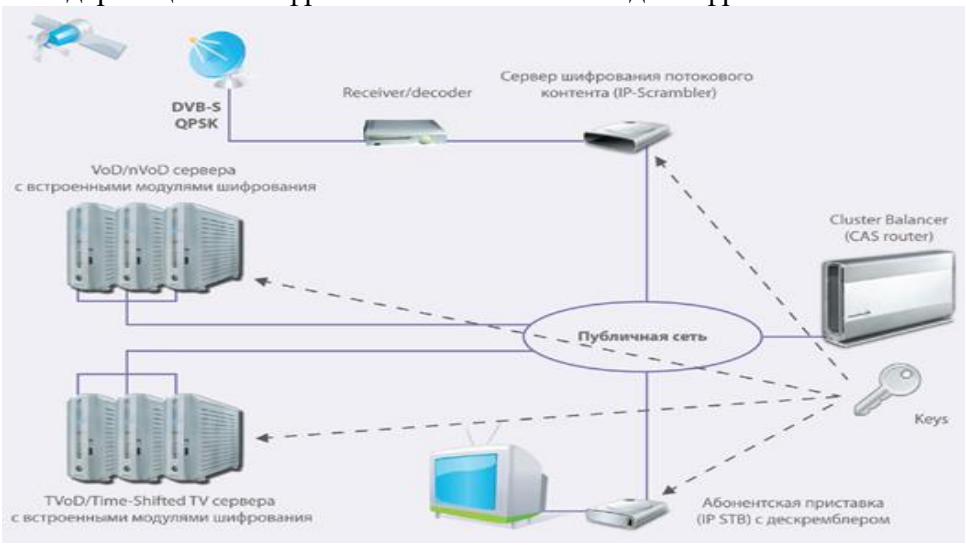
ТЕМА: Система условного доступаIP CAS / DRM.

Система условного доступа NetUP CAS/DRM

Система условного доступа состоит из двух частей - серверной и клиентской. Клиентская часть загружается в IP STB и осуществляет дешифрование потоков. Параллельно ведется процесс обновления ключей с серверной части.

Реализована поддержка приставок от различных производителей, по необходимости возможна адаптация интерфейса абонента к другим типам STB.

Код модуля написан на языке Cc использованием оптимизированных алгоритмов. Код компилируется и работает под платформами x86, PowerPC и др. В случае использования в IP STB операционной системы Linux, модуль загружается в режиме ядра (kernelmodule) и осуществляет перехват пакетов содержащих зашифрованный контент и их дешифрование.



Компоненты системы

Более детально, система состоит из следующих компонентов:

- Модуль ядра Linux на сервере системы сокрытия
- Модуль ядра Linux на абонентском устройстве IP STB
- Клиент-серверное приложение для обмена ключами. Серверная часть запускается на сервере, клиентская часть - на абонентском устройстве IP STB.

Модуль ядра Linux на сервере системы сокрытия перехватывает IP-пакеты с мультимедийным контентом и производит их шифрование. Пакеты помечаются как зашифрованные и перенаправлются далее в сеть. По умолчанию период смены ключей установлен в 10 секунд. Для каждого IP-потока предусмотрена генерация уникальных ключей.

Абонентское устройство устанавливает защищенное соединение с сервером системы сокрытия и периодически получает обновленные ключи шифрования. Полученные ключи передаются в модуль ядра Linux на абонентском устройстве. Данный модуль перехватывает IP-пакеты, получаемые из сети, и производит их дешифрование, если поток зашифрован и имеются в наличии

актуальные ключи для данного IP-потока. Далее дешифрованные пакеты перенаправляются в "приложения", для которых они предназначаются. Данная операция производится "прозрачно" для остальных приложений в IP STB.

Используемая библиотека шифрования имеет сертификат, выданный Федеральной Службой Безопасности (ФСБ) Российской Федерации, подтверждающий соответствие базового алгоритма шифрования стандарту ГОСТ 28147-89 и требованиям к СКЗИ класса КС1.

Электронный сертификат абонента поставляется на любом USB-носителе (флеш-карте). Благодаря сертификату производится надежная идентификация абонента в системе, а так же производится шифрование передаваемой по сети информации.

Рисунок. Абонентское устройство IP STB Aminet 110 с установленным USB-носителем:

Система условного доступа производства компании NetUP позволяет производить шифрование мультимедийных потоков и затем передавать их по незащищенным каналам связи. Только авторизованные абоненты, подписанные на данную услугу, смогут воспроизводить такие потоки. Благодаря системе сокрытия оператор IPTV может четко контролировать доступ к контенту и строить финансовые взаимоотношения с абонентами.

Система условного доступа зарегистрирована в международной организации DVB Project. Назначен идентификационный номер (CAID) – 0x4AEF.

Система поддерживает различное абонентское оборудование: IPTV-приставки (как классические, так и под управлением Android OS) и PC. В зависимости от оборудования, используется соответствующий алгоритм шифрования CSA или AES, который позволит максимально задействовать аппаратные средства для декодирования зашифрованных потоков. Это снижает нагрузку на приставку, что особенно актуально для воспроизведения видео в формате HighDefinition. CSA (CommonScramblingAlgorithm) - общий алгоритм скремблирования, разработанный в 1994 году, продолжает широко использоваться в настоящее время. AES (AdvancedEncryptionStandard) - является одним из самых распространённых на сегодняшний день алгоритмов симметричного шифрования.

Запрос информации

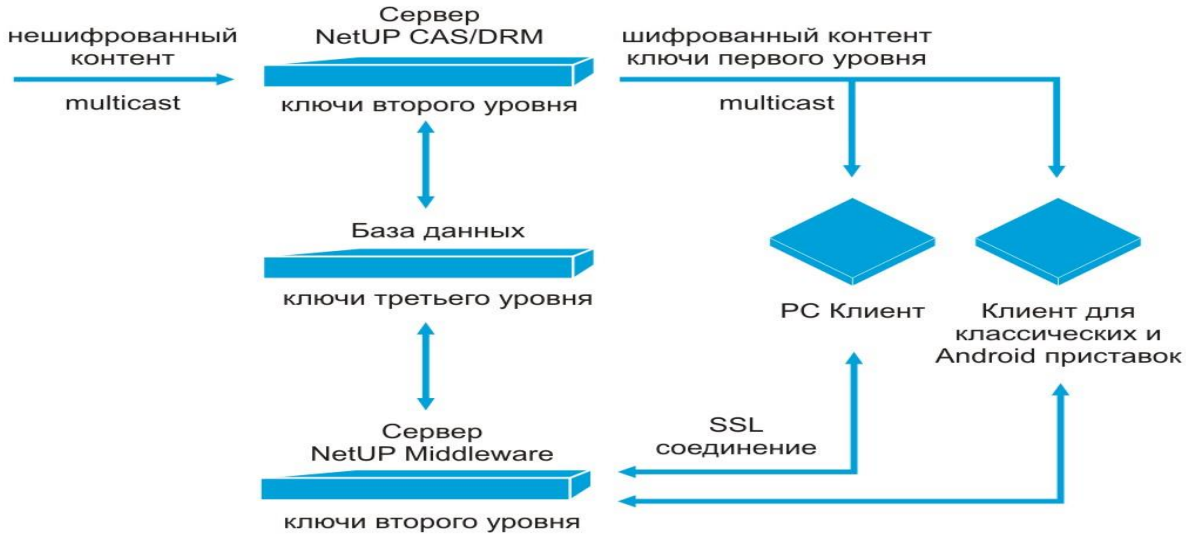


Схема работы система условного доступа NetUP CAS/DRM

Принципы шифрования

С каждой единицей медиа-контента ассоциируется ключ шифрования. В системе NetUP CAS/DRM используется трехуровневое шифрование.

- Ключи первого уровня являются постоянными и выделяются один раз для каждой единицы контента при первом шифровании. Эти ключи хранятся в общей для CAS и Middleware базе данных.
- Ключи второго уровня динамически генерируются на основе ключей первого уровня и текущего времени. Срок жизни ключа второго уровня – 1 час. Так как на серверах CAS и Middleware время синхронизировано, каждый из них может генерировать идентичные ключи второго уровня независимо друг от друга. По запросу ключ второго уровня может передаваться на IP STB, но только для доступных абоненту единиц контента.
- Ключи третьего уровня используются непосредственно для шифрования передаваемых пакетов данных и передаются в зашифрованном виде параллельным потоком вместе с контентом. Ключ третьего уровня генерируется динамически на основании соответствующего ключа второго уровня, IP-адреса и текущего времени. Время жизни ключа третьего уровня – 5 минут.

Механизм аутентификации клиентов в NetUP CAS/DRM

На сервере Middleware в биллинговой системе для каждого абонента создаются лицевой счет, сертификат, приватный ключ и одноразовый код активации. При первом включении приставки или запуске PC клиента, абонент должен ввести выданный ему код активации, после чего на клиентском оборудовании клиента сохраняются сертификат и приватный ключ. Они используются при установке SSL-соединения и аутентификации с сервером Middleware.

В случае, если абонент использует PC клиент, сертификат и приватный ключ при сохранении шифруются исходя из аппаратной конфигурации компьютера, на котором установлен клиент. Это защищает сертификат и приватный ключ от переноса на другие компьютеры. При переносе на другую конфигурацию абонент должен будет ввести новый код активации.

Таким образом, в системе NetUP CAS/DRM отсутствуют смарт-карты доступа, применяющиеся в большинстве систем условного доступа. Это позволяет сэкономить значительные средства на производстве карт.

GOSPELL CAS

Система условного доступа GOSPELL CAS – это аппаратно-программный комплекс, предназначенный для скремблирования транспортных потоков (TS) с целью ограничения доступа абонентов к просмотру ТВ каналов, ведения финансовых политик относительно групп абонентов и

индивидуально, адресной передачи абонентам различной информации и предоставление платных услуг по просмотру ТВ каналов в сети.

Аппаратная часть системы CAS представлена, прежде всего, simulcrypt-совместимым скремблером, который может быть интегрирован на любую цифровую головную станцию сетей CATV: PBI, Sumavision EMR2.1/3.0, Triax TDX, WisiHameleon, TelesteLuminato, и т.д.

Скремблер кодирует в масштабе реального времени выбранные каналы транспортного потока TS. SI/PSI таблицы изменяются согласно алгоритму работы CAS.

Дополнительный поток данных (EMM и ESM), необходимый для работы абонентского приемника (STB: set-topbox), мультиплексируется в выходной транспортный поток TS.

Состав головного оборудования, формирующего транспортный поток TS, стандартен: демодуляторы DVB-S/S2/T/T2/C, DVB-MPEG2/ MPEG4 SD/HD кодеры, оборудование формирования пакетов цифровых каналов (мультиплексоры) и модуляторы транспортного потока для передачи далее в сеть кабельного телевидения (QAM или COFDM-модуляторы).

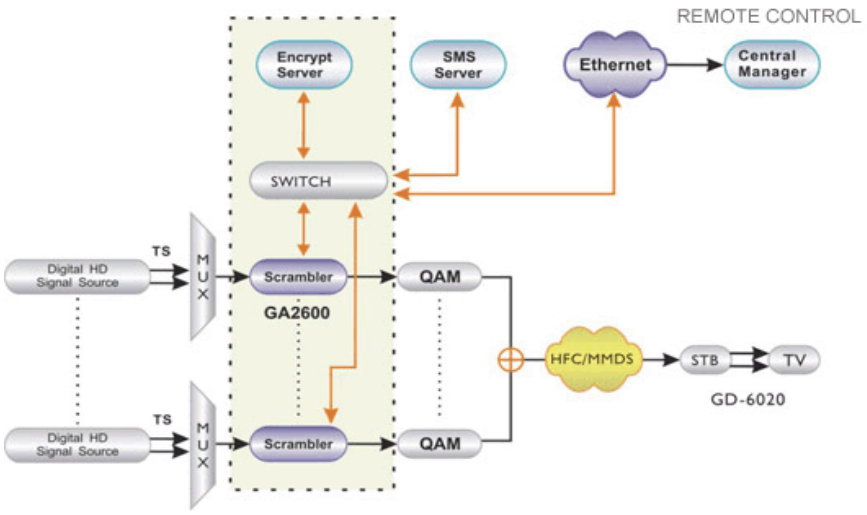
GOSPELL CAS не уступает, например, по своим функциональным характеристикам такой известной системе кодирования, как Conax и очень хорошо зарекомендовала себя в сетях многих операторов Европы и Азии благодаря своей стоимости и функциональности.

GOSPELL CAS установлена и локализована в кабельных сетях Латинской и Северной Америки, Ближнего Востока, Индии и некоторых стран Европы. Система отвечает всем современным стандартам цифровых кабельных сетей, а безопасность и надежность работы системы гарантируют уникальный динамический ключ кодирования и абонентские смарт-карты повышенной криптостойкости (EAL 5+).

Основные функции GOSPELL CAS

- Управление смарт-картами: индивидуально и группами.
- OSD – передача адресных сообщений абоненту (бегущая строка на экране), поддержка русского языка.
- STB-Mail – передача почтовых сообщений абоненту (почтовый ящик в STB), поддержка русского языка.
- IPPT – повременная оплата.
- Привязки смарт-карт: к STB, материнская/дочерняя.
- Чрезвычайное вещание.
- AreaControl – географическая привязка STB и смарт-карт к определенным участкам сети.
- OperatorRestriction – запрет использования STB и смарт-карт из сети другого оператора, также использующего GOSPELL CAS.
- Антипиратские функции.
- Родительский контроль.

Компоненты GOSPELL CAS



CAS Software - основная система, состоящая из модулей ECMG, EMMG, программного обеспечения управления скремблером NMS (NetworkManagementSoftware) и оконечным устройством – STB с IC картой.

Server - управляет программным обеспечением CAS по сети LAN между модулями и устройствами через сетевой коммутатор (Switch).

Switch - обеспечивает обмен информацией между сервером и скремблером по TCP/IP.

Scrambler - кодирует в масштабе реального времени выбранные каналы транспортного потока (TS). SI/PSI таблицы изменяются согласно алгоритму работы CAS. Дополнительный поток данных (EMM и ESM), необходимый для работы абонентского STB, мультиплексируется в выходной транспортный поток TS.

Для обеспечения работоспособности Gospell CAS могут быть использованы любые Simulcrypt совместимые скремблеры. Рекомендуется предварительное тестирование аппаратной части для 100% проверки совместимости. CAS сервер поддерживает работу множества скремблеров.

В состав программного обеспечения комплекса входит:

- CAS (ConditionalAccessSystem) – выполняет адресное кодирование, отправку сообщений и пр. Основные модули: ECMG, EMMG.
- NMS (NetworkManagementSoftware) – программное обеспечение для управления скремблерами.
- SMS (SubscriberManagementSystem) – система управления реестром абонентов, хранящая и обрабатывающая сведения для системы адресного кодирования.
- EPG (ElectronicProgramGuide) – система создания и отправки программ телепередач цифровых каналов на абонентские STB, а также для удаленного обновления программного обеспечения самих STB, которое будет произведено, как только он будет включен.

Все программное обеспечение устанавливается на сервере и имеет возможность удаленного подключения и управления по сети.

В качестве СУБД для GOSPELL CAS используется MS SQL Server, что является чрезвычайно удобным и выгодным решением для операторов, т.к. в рамках данной СУБД существует бесплатная версия SQL Express, которая позволяет реализовать все возможности GOSPELL CAS. Единственным ограничением бесплатной версии является объем базы данных (БД) – до 4ГБ, что с избытком покрывает потребности оператора CATV.

Отдельно следует отметить наличие CAM модуля GOSPELL CAS для современных телевизоров с CI слотом. В этом случае абоненту нет необходимости приобретать STB, т.к. декодирование программ будет осуществляться непосредственно в телевизоре.

Таким образом, на постсоветском пространстве уже достаточно много внедрений цифровых систем Телесте, особенно бурно они проходили в последние два года. Это доказывает, что продукт соответствует современным требованиям, а выбор его известными компаниями означает надёжность и проверенность.

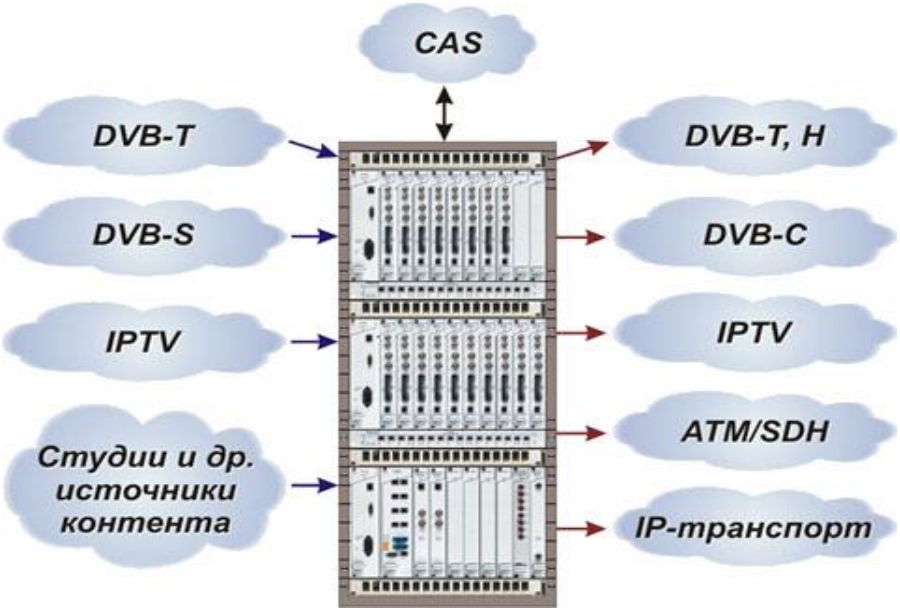


Рисунок. ATMux и взаимодействие с различными технологиями доступа и доставки контента

DVB решение Teleste способно принимать контент в различных форматах, см. рис.1, взаимодействовать с системами условного доступа CAS открытых стандартов, обеспечивать вещание в различных форматах, в т.ч. DVB-C, -T, -H, IPTV, а также обеспечивать передачу контента по глобальным сетям ATM/SDH или IP. Такая способность легко интегрироваться с глобальными сетями позволила многим компаниям, в числе которых ComHem (Швеция), реализовать крупные сети государственного масштаба.

Один из вариантов использования цифровой станции Teleste по ATM сетям. Концепция этого решения заключается в коммутации сервисов (ТВ и радиоканалов) и услуг по технологии ATM, для этого используется коммутатор ATM Presto. Коммутатор Presto способен обрабатывать сервисов до 2,5 Гбит/с, что эквивалентно 600-700 ТВ-каналам стандартного разрешения в MPEG-2. Также в системе используются 2 ключевых элемента:

- Staccato – входное устройство, обеспечивающее приём и подготовку контента для дальнейшей обработки.
- Legato – выходное устройство, обеспечивающее необходимую для провайдера обработку контента.

Обобщённая схема построения системы показана на рисунке.

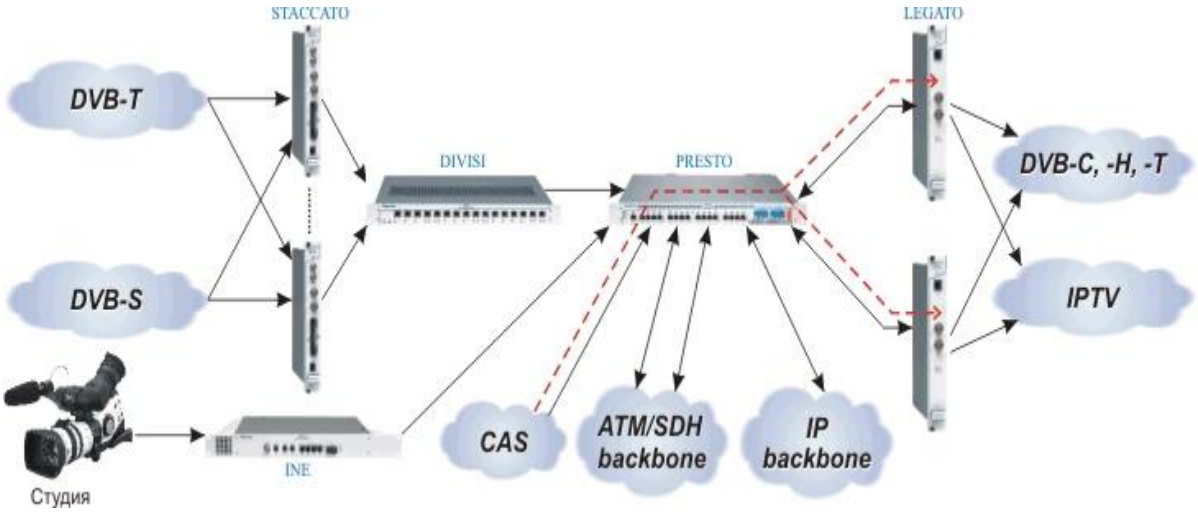


Рисунок Обобщённая схема цифровой станции

На данной схеме показаны дополнительные элементы:- INE – MPEG-2 4:2:0 encoder с ATM-выходом;- DIVISI – интеллектуальная патч-панель с 16-ю входами/выходами STM-1 для объединения большого количества Staccato или Legato.

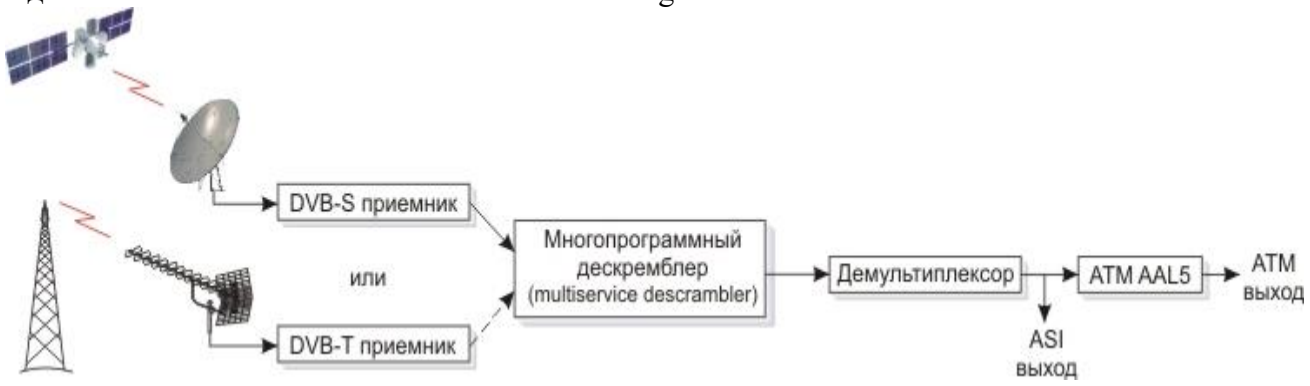


Рисунок. Блок-схема Staccato

Как видно из рисунка, Staccato является универсальным модулем, трудно подобрать ему аналог. Его можно использовать для получения любого контента за исключением, пожалуй, контента, принимаемого из студий в несжатом виде. В таком случае необходимо применять encoder INE. Staccato обладает следующими основными функциями:

- демодуляция сигнала при приёме со спутника DVB-S или из эфира DVB-T;
- дескремблирование 1 или 2-х закрытых каналов благодаря наличию 2-х CI, однако при необходимости и при использовании PRO CAM и соответствующей смарт-карты Staccato способен открывать и большее количество каналов, это возможно благодаря опции multiservicede-scrambling;
- наличие ASI-входа и выхода;
- демультиплексирование необходимых потоков до SPTS;
- инкапсуляцию сервисов на ATM-выход в нужных VPI/VCI;
- несколько полезных опций: сканирование сервисов во входном потоке, PSI/SI мониторинг и т.д.;
- интеграция с IP-решениями, например, при помощи iGATE.

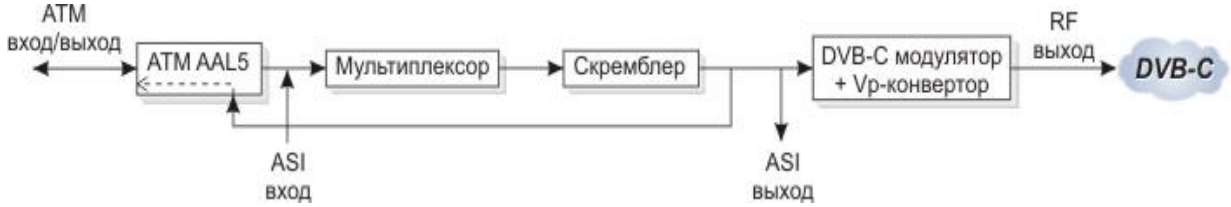


Рисунок. Блок-схема Legato

Legato также является универсальным модулем, который обрабатывает и закрывает, шифрует контент для сетей DVB и IP, что является крайне важной задачей на стыке технологий.

Legato обладает следующими функциями:

- получение необходимых сервисов через ATM AAL 5 или ASI-вход;
- мультиплексирование сервисов;
- скремблирование, в т.ч. и multiscrambling (все известные системы);
- выдача сформированных потоков на ATM AAL 5, ASI-выход и через DVB-C модулятор со встроеннымup-конвертором в сеть CATV или MMDS;
- другие дополнительные функции, например, PSI/SI insert;
- интеграцию с IP-решениями, например, через iGATE или iPLEX.

Одним из самых важных преимуществ такого универсализма является адаптируемость устройства к различным задачам.Зачастую оператор или провайдер услуг не может спрогнозировать на перспективу, какой функционал устройства ему может понадобиться, и, как

правило, приобретает изделия с минимальным функционалом, что безусловно отрицательно сказывается на масштабируемости, гибкости решения и защите инвестиций.

Использование Staccato и Legato позволяют избежать такой ошибки. Оператор может заказать любую необходимую в данный момент комплектацию, однако впоследствии может дозаказать дополнительные опции, активируя их посредством электронного ключа, что в условиях действующего комплекса довольно удобно.

Эта особенность позволяет, например, в крупных сетях использовать полнофункциональные Legato для формирования и шифрования контента в одном месте – на центральной головной станции (ЦГС), а на удалённых сайтах - подголовных станциях (ПГС) использовать Legato с ограниченным функционалом, например, как интерфейс ATM -> DVB-ASI, что позволит значительно сократить вложения, не ограничивая развитие в перспективе.

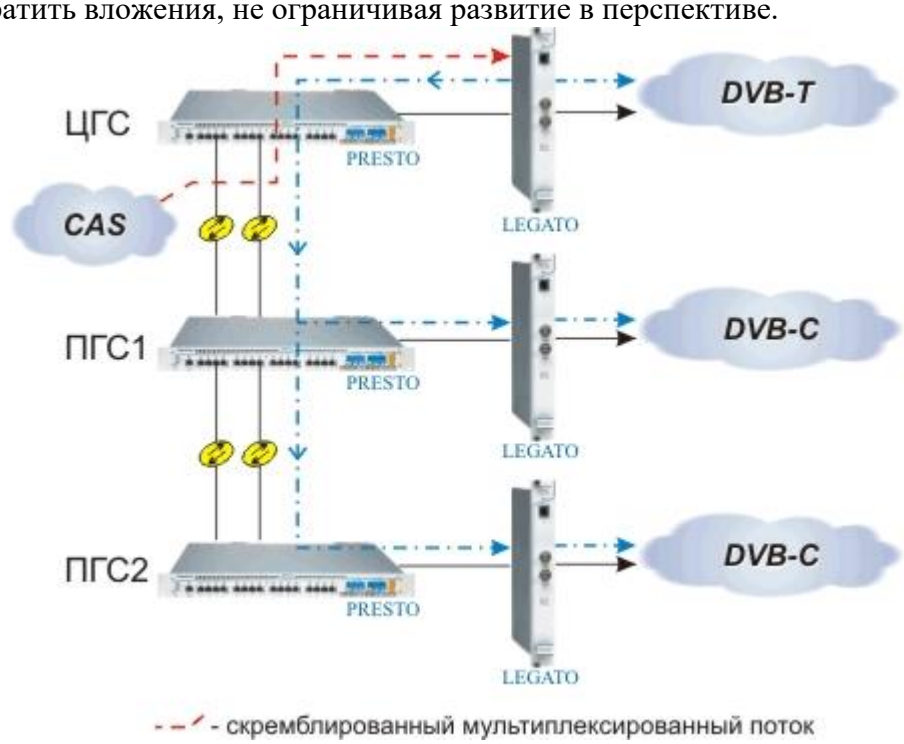


Рисунок. Распределённая система условного доступа CAS

Концепция построения цифровой станции Teleste позволяет:

- минимизировать количество активных элементов, что повышает надёжность работы системы, уменьшает размеры и энергопотребление, минимизировать количество соединительных кабелей в системе;
- центральное управление системой, канал управления размещается в том же физическом интерфейсе, что и сервис, но как отдельная пара VPI/VCI, это позволяет не заботиться о развёртывании дополнительных кабелей и каналов управления;
- не требуются дорогостоящие ASI-матрицы для обеспечения резервирования элементов и бесперебойного предоставления сервисов, роль матрицы выполняет ATM-коммутатор Presto;
- универсализм Staccato и Legato позволяет интегрировать их в любые сети, использовать их для любых сервисов и в любых технологиях, что особенно актуально в настоящее время – время сосуществования технологий различных идеологий: DVB, IP, ATM и др.

Таким образом, основными достоинствами цифровой станции Телесте можно назвать:

- универсализм элементов и самой системы в целом;
- интеграция в сети DVB и IP;
- высокая надёжность, связанная с минимизацией каблирования, наличием коммутатора, реализующего возможности резервирования, малого количества активных элементов;
- управляемость системы.

4. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бубнов А.А. Основы информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования. - 3-е изд., стер. - М.: Академия, 2017. - 256 с.
2. Бернет С. Криптография. Официальное руководство RSA Security = RSA Security'sOfficialGuidetoCriptographi / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. - 2-е изд., стер. - М. : БИНОМ, 2017. - 381 с.
3. Зайцев А.П. Техническая защита информации М. Горячая линия-Телеком, 2018.- 616с.
4. Ищейнов, В.Я. Информационная безопасность и защита информации: словарь терминов и понятий: словарь / Ищейнов В.Я. — Москва: Русайнс, 2019. — 226 с.
5. Касперски Крис Компьютерные вирусы изнутри и снаружи / Крис Касперски. – СПб.: Питер, 2018. – 526 с.
6. Корнеев И.К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов. - М. : Проспект, 2018. - 333 с.
7. Краковский Ю.М.Информационная безопасность и защита информации : учеб. пособие / Ю. М. Краковский. - М. ; Ростов н/Д : МарТ, 2017. - 287 с.
8. Крылов, Г.О. Базовые понятия информационной безопасности: учебное пособие / Крылов Г.О., Ларионова С.Л., Никитина В.Л. — Москв : Русайнс, 2020. — 257 с.
9. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества: монография / Кузнецова А.В., Самыгин С.И., Радионов М.В. — Москва: Русайнс, 2020. — 118 с.
10. Куприянов А.И.Основы защиты информации : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. : Academia, 2017. - 256 с.
11. Мельников В.П. Информационная безопасность [Текст] : Учебник / В. П. Мельников, А. И. Куприянов; Под ред.В,П. Мельникова. - 2-е изд., перераб. и доп. - М. : Академия, 2020. - 268 с.
12. Олифер В.Г. Сетевые операционные системы СПб: Питер, 2016.
13. Сингх С. , Книга шифров. М.: «Издательство Астрель», 2016 г.
14. Таненбаум Э., Компьютерные сети СПб.:Питер, 2016.
15. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с.

Дополнительные источники:

1. С.В. Дворянкин, Д.В. Девочкин "Методы закрытия речевых сигналов в телефонных каналах" “Конфидент”, №5 июль-сентябрь 2015г
2. Киреев С.Ф., Макевнин А.А. Противодействие средствам иностранной технической разведки в СВЧ- и ИК-диапазонах длин волн. Учебное пособие. 2016.
3. Мельников В.П. Информационная безопасность М.: «Академия», 2017, 336с.
4. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений СПО. – М.:ФОРУМ: ИНФРА – М, 2018.
5. В.В. Фомин, В.Н. Дудник, В.Е. Лепин, Т.В. Батенева, М.С. Подлубный "Способ кодирования речевых сигналов для устройств радио-и телефонной связи" -Сб “Техника радиосвязи”, вып 3 2017г.

Интернет-ресурсы:

1. Образовательный портал - http://www.edu.ru;
2. Интернет университет информационных технологий - http://www.intuit.ru;
3. Центр информационной безопасности - http://www.bezpeka.com

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

Группа 51 РРТ

ЖУРНАЛ ОТЧЕТОВ
по выполнению лабораторных работ
профессионального модуля
ПМ 03. Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

по специальности
11.02.10 Радиосвязь, радиовещание, телевидение (углубленной подготовки)

ВЫПОЛНИЛ _____ /_____/

ПРИНЯЛ _____ /Рачинский С.А./

Белгород 2019 г.