Защита цифрового спутникового телевидения от нелегального просмотра.

Вообще, цифровое спутниковое телевидение во многом схоже с широковещательным. Это беспроводная система доставки телевизионного сигнала непосредственно в дом к пользователю. И широковещательные ,и спутниковые станции передают информацию, используя радиосигнал.

В Москве и Московской области можно принимать сигналы с более, чем 10 спутников. Например, (наиболее популярные) **Hot Bird** (более 560 каналов), **Sirius** (около 90 каналов), **Astra** (более 300) и **Eutelsat W4** (НТВ Плюс и еще около 10 каналов).

Радиосигнал со спутника ,в принципе, может быть принят любым желающим в территории вещания спутника независимо от желания передающей стороны. Однако в большинстве случаев телекомпания - владелец программы заинтересована в пресечении нелегального приема, например, при передаче программ платного телевидения, деловых телеконференций, или в ограничении территории, на которой можно принимать данную программу по условиям авторского права. Самым популярным способом ограничения доступа является засекречивание передаваемых программ (шифрование сигнала) таким образом, чтобы сделать прием невозможным без специального декодера, предоставляемого провайдером. На практике используется восемь систем кодирования для **PAL/SECAM**, четыре для **NTSC** и шесть для сигнала **MAC**. К примеру , **Viaccess** ,**Irdeto**, **Betacrypt**, **Nagravision**. И, чтобы смотреть любимую программу придется приобрести карточки, ресивер и вносить абонентскую плату.

Перейдем непосредственно к шифрованию сигнала. Основные требования к такой системе шифрования - она должна быть недорогой, надежной, причем качество сигнала при этом не должно ухудшаться. Первое требование очевидно и означает, что стоимость декодера не должна существенно влиять на стоимость всей приемной установки. Высокая надежность предполагает, что требуется специальное устройство - декодер, который, по крайней мере, не может быть изготовлен в домашних условиях и содержит ключ или специальную карту, защищенные от копирования.

Самый простой метод защиты - искажение синхросигнала так, что стандартный телевизионный приемник не может восстановить изображение, оно появляется на экране в виде отдельных полос или сегментов. Информация о синхросмеси передается в сигнале в скрытой форме и обнаруживается декодером, который восстанавливает стандартные синхроимпульсы. Более высокая надежность достигается добавлением инвертирования части сигнала, смещением его уровня. Еще более сложный путь - сдвиг во времени отдельных строк изображения, или рассечение строк и перестановка местами рассеченных частей, или перестановка местами строк.

В одной из первых использовавшихся в Европе систем вместо строчного синхроимпульса подставлялся пакет синусоидальных колебаний с частотой 2,5 МГц, применялись также различные варианты инвертирования изображения. Разновидность этого метода под названием **Irdeto/Luscrypt** используется при кодировании программы **RTL-4** на спутнике **Astra**. Схожий результат получается при передаче цифровых звуковых сигналов в интервале обратного хода луча, используемой Европейским вещательным союзом в системе "Евровидение". Цифровой пакет нарушает структуру строчного синхроимпульса и сбивает работу амплитудного селектора, поэтому на приеме необходимо специальное устройство регенерации синхросмеси.

Системы со смещением уровня отдельных компонентов видеосигнала оказались не очень надежными и постепенно от них отказались в пользу более совершенных методов со смещением во времени отдельных элементов изображения, которые обеспечивают значительно более высокую надежность. Среди систем, позволяющих распознать изображение, но затрудняющих его просмотр наиболее известна **Discret**, где изображение каждой строки задерживается на 0,1 или 2 мкс с помощью дополнительных аналоговых линий задержки, подключаемых к каналу на период строки по псевдослучайному закону. На приемной стороне закон чередования восстанавливается по кодовому слову, передаваемому совместно с сигналом и расшифровываемому декодером.

Videocrypt

В системе **Videocrypt** кодер рассекает каждую строку в одной из 256 точек, выбранных по псевдослучайному закону, и меняет местами части рассеченной

строки. При этом полностью разрушается структура изображения по вертикали, но частично сохраняется горизонтальная структура - титры, надписи, меню программ Информацию, необходимую для восстановления изображения, декодер получает из двух источников: один ключ передается в закодированном виде в интервале кадрового гасящего импульса, другой распространяется в виде специальной абонентской карточки, рассылаемой подписчикам периодически. **Videocrypt** - наиболее распространенный метод кодирования ТВ сигналов, передаваемых в системе **PAL**.

Nagravision

Более сложная система **Nagravision** требует на приеме памяти объемом в полукадр. Изображение на передающей стороне записывается в буфер и передается построчно, но с перемешиванием порядка строк по псевдослучайному закону. На приеме операции производятся в обратном порядке. В системе **Nagravision** вертикальная структура изображения не нарушается, но любая горизонтальная полоска как бы размазывается по всему экрану. Эта система в свое время была выбрана в качестве основной испанскими вещательными компаниями.

Syster

Метод кодирования по системе **Nagravision** требует наличия в декодере цифровых микросхем памяти, объема которых достаточно для запоминания информации и полукадре, что заметно повышает стоимость декодера. Для ее снижения была разработана модификация метода (**Syster**), в которой строки в полукадре разделены на шесть блоков и перемешивание строк осуществляется внутри каждого блока. Это усовершенствование позволило уменьшить объем необходимой памяти и в конечном счете удешевить декодер. Для авторизации (опознавания) декодера применяется специальный ключ со встроенной микросхемой, аналогичной карточке в системе **VideoCrypt**. Система кодирования изображения **Syster** используется на российских спутниках ГАЛС-1, -2 (36°E). Ее также использует крупнейшая вещательная компания Франции Canal Plus для передачи программ через спутник **Telecom HB**.

Videocipher II

Все применяемые на североамериканском континенте системы засекречивания имеют общую особенность, повышающую их надежность: абонентский декодер работает в интерактивном режиме и активизируется только когда, когда получает от центра управления соответствующую команду. В наиболее распространенной системе **Videocipher II**, разработанной компанией ***General Instruments*** из видеосигнала полностью удаляются обычные сигналы синхронизации, полярность сигнала инвертируется, а сигналы цветового опознавания переносятся на нестандартную частоту.. Обычный ТВ приемник не может принять такой сигнал, и требуется установка специального декодера. Каждому декодеру присвоен индивидуальный номер ,и при включении он посылает свой номер по телефонным линиям в центр управления компании ***General Instruments***, где он опознается и по спутниковому каналу подается специальное сообщение санкционирующее прием и содержащее инструкции по декодированию. Таким способом практически исключается использование "пиратских" декодеров.

Сигналы двух звуковых каналов в системе **Videocipher II** передаются в цифровом виде совместно с сигналами синхронизации и другой служебной информацией в интервале строчного гасящего импульса. Аналого-цифровое преобразование осуществляется с точностью 15 бит/отсчет, что обеспечивает динамический диапазон звучания более 75 дБ (теоретически 92 дБ).

В связи с широким распространением стандарта **D2-MAC** в спутниковом вещании возникла необходимость кодирования телевизионных сигналов этого стандарта. В системе **D2-MAC** яркостные и цветоразностные компоненты изображения передаются отдельно, поэтому рассечение и перестановка этих компонент также осуществляются раздельно. Эта система, получившая название **EuroCrypt**, широко используется на спутниках **SIRIUS** (5,2°E), **TELE-X** (5°E), **INTELSAT-707** (1°W), **THOR-1** (0,8°E), **TV SAT-2** (0,6°E). Для системы кодирования **EuroCrypt** разработаны два способа: перестановка компонент с двухкратным рассечением и перестановка компонент цветоразностного сигнала. В первом случае обеспечивается больший уровень засекречивания, сигналы яркости и цветности разрезаются каждый в некоторой точке и компоненты их

переставляются местами. Место рассечения изменяется по псевдослучайному закону независимо для каждой компоненты

Для расшифровки на приеме используется абонентская карточка с вмонтированным в нее кристаллом памяти, в которой записаны ключи к коду и инструкции по дешифровке. **Eurocrypt** применяется более чем в 80% всех ТВ каналов, использующих сигналы **D2-** и **D2-MAC**.

Засекречивание сигналов в цифровом телевидении не представляет особой проблемы, здесь может широко использоваться весь арсенал методов, разработанных ранее для цифровой радиосвязи. В одной из практически реализованных систем цифровой поток зашифровывается с помощью передаваемого вместе с сигналом кодового слова длиной 56 бит, генерируемого псевдослучайным образом и сменяемого с интервалом от долей до нескольких секунд Кодовое слово в свою очередь зашифровывается с помощью ключа, обновляемого раз в несколько недель, а тот последний рассылается абонентам по спутниковому каналу также в засекреченном виде Алгоритм декодирования записывается в кристалле микропроцессора, помещаемом либо в декодере, либо в абонентской карточке и работающем только при наличии ключа. Степень секретности такого кода весьма высока.

Абонентские карты свои пароли наружу не выдают. Но сами они раскодировать видеопоток тоже не могут - не хватает мощности. Поэтому декодирование проводится в два этапа. Карточка вставляется в специальный блок тюнера - **CAM** (***Conditional Access Module***, модуль условного доступа). При приеме кодированного канала **CAM**-модуль транслирует карте всю служебную информацию, идущую на канале параллельно видеосигналу (примерно как телетекст). На закрытых каналах в этой информации есть, среди прочего, и схема восстановления телесигнала. Эта схема зашифрована, и вот именно для ее расшифровки в смарт-карте есть ключи. Получив от **CAM**-модуля такую схему, карта расшифровывает ее собственным процессором и возвращает назад. А **CAM**-модуль, который часто называют декодером, с помощью этой расшифрованной схемы восстанавливает телесигнал.

Схемы восстановления передаются каждые десять-пятнадцать секунд. Но зашифрованы они одним ключом, который хранится в смарт-карте и меняется

гораздо реже вещателем канала. Пока карта вставлена в работающий тюнер, ей транслируется вся служебная информация, идущая на канале параллельно обычной картинке. Либо со спутника, если тюнер с **CAM**-модулем подключен к спутниковой антенне. А если это тюнер кабельной сети - тогда через кабель.

Современная смарт-карта - это маленький компьютер, и если вещатель передает ей по служебному каналу команду, то карта ее «видит» и послушно выполняет. Это называется «управление через эфир». Так можно посылать новые ключи для декодирования каналов - карта их запомнит и будет использовать. Кроме того, через эфир можно просто включать-выключать карточки.

Команды повторяются круглосуточно (к примеру, если тюнер во время передачи команды выключен), и даже если зрителей сотни тысяч, цикл обращений ко всем их карточкам проходит за десятки минут. Многие даже не знают о них. Все максимально упрощено: купил карточку, вставил, включил. Остальное сделает **CAM**-модуль, что в общем-то правильно.

И заканчивая, этот обзор по защите спутникового телевидения, можно добавить, что в будущем, конечно же , будут разрабатываться и использоваться более новые системы шифрования видеопотока.

Используемые ссылки и литература:

1. Статья “Защита телеканалов и возможность ее преодоления” -

(http://www.computerra.ru/offline/2002/469/21579/print.html)

2. Статья “Засекречивание ТВ сигнала” -

(http://www.smolsat.com/secret.html)

3. ‘A basic intro to VideoCrypt ‘

(http://www.heyrick.co.uk/willow/vcrypt.html)\

4. Системы кодирования спутниковых каналов

(http://sat-tv.infonet.by/kod.htm)