взлом телевизоров вблизи и на расстоянии

крис касперски aka nezumi aka elraton aka souriz aka жирный нутряк ибн мыщъх, no-email

все мы используем пульты дистанционного управления на ИК основе, но далеко не каждый знает какие возможности и опасности они предоставляют. помимо "несанкционированного" переключения каналов у соседа, хакер может проникнуть в инженерное меню, чудовищно исказив геометрию экрана, отключив развертку, или убив телевизор каким-нибудь другим способом

введение

Как сказал Пелевин: телевизор это унитаз, только наоборот — в унитаз серем мы с вами, а из телевизора серут на нас, причем во всей физической прямоте этого слова. Но даже не это самое страшное (г. не грязь, высохнет — само отвалится), фактически, телевизор превращается в пульт дистанционного управления телезрителем, являясь не просто одним из методов организации видеоряда, а основой телевещания — главным способом воздействия рекламно-информационного поля на сознание, при которой телезритель становится телепередачей, управляемой дистанционно. И в этом состоянии он проводит значительную часть своей жизни.

Хакеры телевизор вообще не смотрят, да и другим не советуют. А самые радикальные группы анархистского толка даже объявляют телевизорам священную войну aka~~, то есть~~ джихад. Помните того пацана, который, оставшись один дома (фильм "home alone"), с помощью нехитрого устройства~~приспособления~~, сооруженного из пульта дистанционного управления, соединенного с телескопом, мешал "любимой" соседке смотреть телевизор, постоянно переключая каналы? Уверен, многие пытались повторить его подвиг, но ~~достичь~~ успеха достигли лишь ~~удалось~~ единиц~~ам~~ы. Хотите ~~у~~знать почему?

Оставив морально-юридический аспект вопроса догнивать на помойке, возьмем свой собственный телевизор и попробуем извратиться с ним по полной программе. Посмотрим, как далеко мы сможем зайти и что у нас получится с ним сделать.

боевая экипировка

Для дистанционного управления телевизором нам потребуется пульт, совместимый с типом атакуемой жертвы на уровне протоколов модуляции и команд управления. Систем ИК-связи всего ~~модуляции всего~~ три:

- **система ITT**, разработанная компанией GRUNDIG, и основная на измерении интервалов времени между последовательности коротких импульсов излучения (в настоящее время практически полностью вышла из употребления);
- **система RC-5**, разработанная компанией PHILIPS, и использу~~я~~ющая метод двухфазной передачи данных, модулирующий постоянный несущий сигнал (используется и по сей день, но все реже и реже, да и то в основном в отечественных телевизорах);
- **система SIEMENS**, разработанная одноименной компанией, и модулирующая высокочастотный несущий сигнал (частота которого, кстати говоря, может варьироваться в широких пределах) навороченным цифровым протоколом, поддерживающим среди прочих фич еще и синхронизацию приемника с передатчиков и пользующейся большой популярностью у зарубежных телестроителей.

В настоящее время чаще всего используется объединенная система RC-5+SIEMENS, реализованная в микросхемах практически всех популярных производителей: PHILIPS, SIEMENS, THOMSON, SAMSUNG, LG и др. Теоретически вполне возможно создать универсальный пульт, поддерживающий множество моделей телевизоров одновременно и такие пульты уже представлены на рынке (изготовленные, как правило, кустарным способом). Если же такого пульта нет, необходимо приобрести "родной" пульт модели-жертвы, которые сейчас продаются практически в любом магазине, торгующим теле-аудио техникой.

По паспорту, номинальный рабочий диапазон пульта редко превышает несколько десятков метров (да и то, лишь на свежих батареях). Учитывая невысокую плотность расположения домов, для диверсионных целей такого поражающего радиуса оказывается крайне недостаточно и без серьезной "хирургической" доработки здесь не обойтись! Можно,

конечно, приложить пульт к окуляру телескопа типа TAL-100R~~"Мицар" или "Альтаир"~~, выпускаем~~ых~~ого Новосибирским Приборостроительным Заводом, и, прицелившись через искатель (это вспомогательная подзорная труба на телескопе такая с перекрестьем), вести огонь прямой наводкой, расстреливая телевизоры в домах напротив. Однако тут надо учесть, что коэффициент преломления инфракрасных лучей заметно отличается от видимого света и визуальная фокусировка становится невозможн~~а~~ой! Необходимо выполнить перерастет (учите матчатсь!) или подобрать положение фокусировочного кольца экспериментально. Но все равно, телескоп — это дорого, громоздко и неудобно. Гораздо проще (и дешевле) доработать сам пульт, а для этого его необходимо вскрыть, орудуя кухонным ножом как показано на рисунке 1.

Рисунок 1 трепанация пульта дистанционного управления

После извлечения печатной платы из корпуса мы увидим излучающий инфракрасный светодиод, один из выводов которого, как правило, подключается к общему проводу (то есть, к массе), а другой — к коллектору биполярного высокочастотного транзистора. Предельную яркость ограничивает резистор, подключенный к базе (см. рис. 2).

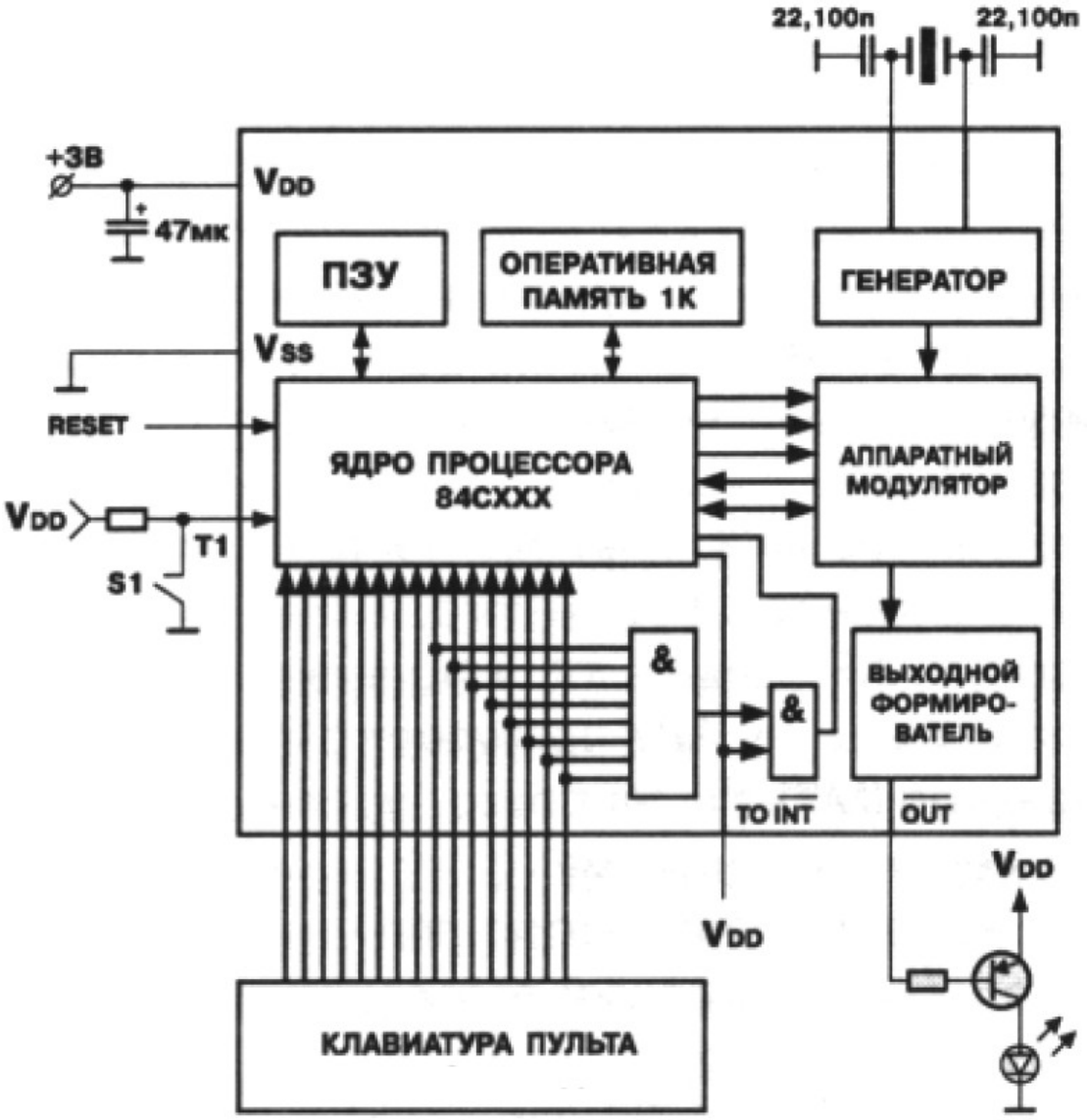

Рисунок 2 структурная схема типового пульта дистанционного управления

Уменьшив сопротивление "базового" резистора (например, подпаяв параллельно ему еще один), мы увеличим яркость свечения светодиода и "дальнобойность" пульта резко возрастет. Любители экстремальных ощущений могут перерезать питающую дорожку, ведущую к эммитору и подать на транзистор до 5 Вольт или даже немногим больше того. Светодиод заморгает как сумасшедший и хотя он скоро сгорит, за это время с таким пультом можно успеть многим навредить, хотя это будет не хакерство, а самое настоящее варварство.

Серьезные охотники удаляют светодиод, заменяя его лазерным излучателем. Лазерные указки — самое доступное оружие, но — увы — далеко не самое лучшее, поскольку их рабочий диапазон лежит в видимом свете, а фотоприемник телевизора защищен инфракрасным светофильтром, значительно ослабляющим видимый свет, поэтому потребуется достаточно мощная указка, для "раскачки" которой одного транзистора может уже не хватить и придется подпаивать дополнительный каскад, а для этого необходимо не только владеть навыками пайки, но и иметь некоторые познания в электронике.

Сторожевые системы (которые легко найти в магазинах, торгующих радио-конструкторами или заказать по почте) зачастую используют инфракрасные лазеры, идеально подходящие для охотничьих целей. В зависимости от фантазии и умения работать руками (по металлу) конструкции орудия могут быть самыми различными. Кто-то засовывает лазерный излучатель прямо в ствол пневматической винтовки, кто-то вытачивает специальную насадку на бинокль или подзорную трубу, юстируя ее так, чтобы центр "креста нитей" окуляра совпадал с инфракрасным лучом. Работает такое устройство практически на любых расстояниях, фактически ограниченных одним лишь горизонтом видимости, однако, если требуется

пострелять в жильцов, живущих снизу или снизу, то… ничего не получится. Разве что забраться на крышу соседнего дома или... подобрать только что выпаянный светодиод и прикрепить его к телескопической штанге (сооруженной из антенны старого радиоприемника, например), которую охотник сможет двигать во всех направлениях.

Достоинство светодиода (по сравнению с лазером) в том, что он дает расходящийся пучок света, многократно переотражаемый от предметов окружающей обстановки (никто из вас не пробовал управлять телевизором направив пульт в потолок или противоположную стену?), поэтому "подстрелить" жертву становится очень легко — даже не обязательно прицеливаться. Главный (и, пожалуй, единственный) минус такого решения в том, что интенсивность изучения убывает пропорционально квадрату расстояния, в то время как лазер дает практически параллельный пучок. Короче, залогом успешной охоты становится богатый инвентарь. В одних случаях применяется одно оружие, в других — другое.

мелкие пакости

Итак, вражеский телевизор лежит в перекрестье прицела, влажные от волнения пальцы застыли на пульте. Самое простое, что можно сделать (не привлекая к своей персоне никакого внимания) — нащупать большую красную кнопку и вдавить ее до упора, отправляя телевизор в ждущий режим типа standby. После нескольких таких самопроизвольных отключений, агрегат, как правило, отправляется хозяевами на лечение в ближайшую мастерскую (очень помогает против соседей, увлекающихся повышенной громкостью по ночам, когда все нормальные хакеры занимаются отладкой программ, требующей глубокой сосредоточенности, граничащей с медитацией и все посторонние звуки высаживают на глухую измену, то есть раздражают). Еще можно проиграться переключателем каналов, кнопкой "mute", регуляторами яркости, насыщенности и контраста, но, поскольку, все эти действия отображаются на экране, жертва быстро сообразит чья тут собака порылась и займется поисками охотника, наблюдая за окнами соседних домов. Так что, дабы не быть пойманным и растерзанным без суда и следствия, необходимо заблаговременно позаботиться о маскировке.

Некоторые хакеры практикуют совершенно изумительный трюк — включая телевизор в отсутствие хозяев, они запускают режим "ручного" поиска станций и заводят все каналы на "пустоту". Внешне это выглядит так, как будто-то телевизор "теряет" каналы, что можно быть вызвано, например, выходом из строя микросхемы энергонезависимой памяти, программатора или фильтров в цепях питания. Дефекты подобного рода встречаются достаточно редко, но относятся к разряду "трудных" и телемастер может ковыряться в телевизоре целый месяц, прежде чем придет к выводу, что источник сбоев приходит откуда-то извне. Но по сравнению с тем, что ждет нас впереди, это всего лишь невинные шалости. В конце концов, каналы можно настраивать каждый раз перед просмотром.

С телевизорами, имеющими парольную защиту от детей, все обстоит намного хуже. По умолчанию она не задействована и хакер свободно может установить любой пароль, предварительно заблокировав доступ ко всем органам управления. Подобрать пароль за разумное время практически невозможно и для снятия блокировки приходится перепрограммировать микросхему энергонезависимой памяти, а для этого необходимо иметь фирменную прошивку, которая есть только в крупных сервисных центрах, да и то не во всех, но даже если ее раздобыть (контрабандой или считыванием с телевизора идентичной модели), все индивидуальные настройки, касающиеся фокусировки, геометрии, цветового баланса и даже разгонных напряжений кинескопа окажутся безвозвратно утерянными и качество изображения резко упадет. Теоретически, все параметры можно отстроить заново, но далеко не каждый мастер захочет с этим возиться, да и невозможна такая настройка в условиях маленькой мастерской. Без специальных (и весьма дорогостоящих) генераторов сигналов здесь не обойтись, а, значит, после ремонта о прежнем качестве можно и не мечтать. (*Небольшая ремарка: среди телемастеров так же встречаются хакеры, которые знают где именно хранится пароль и как он обнуляется, но таких еще найти надо*).

Кстати говоря, огромным достоинством большинства телевизоров SAMSUNG является автоматическая загрузка базовой прошивки из ПЗУ: достаточно установить чистую микросхему памяти (как правило, марки IC902), включить телевизор в сеть и оставить его в ждущем режиме на 10…15 сек., но при этом вместе с прошивкой переписываются и настройки по умолчанию, то есть для достижения качественного изображения, их все равно придется перенастраивать заново.

внутри инженерного меню

Практически все современные телевизоры (DVD-плееры и прочие устройства) имеют специальное инженерное меню (service menu), дающие доступ к настройке служебных параметров (фокусу, геометрии экрана, цветовому балансу, etc) и скрытым возможностям типа HOTEL MODE (режим "отеля") – очень полезный режим для телевизоров, установленных в гостиницах или мотелях, который блокирует все функции пульта управления, кроме переключения каналов, а при необходимости еще и ограничивающий максимальную громкость звука, чтобы она никому не мешала. Только представьте как обрадуется владелец телевизора с заблокированным пультом и громкостью, сбавленной до нуля. А ведь разблокировать все назад можно только в мастерской!

Вызов инженерного меню как правило осуществляется недокументированной комбинацией клавиш штатного пульта дистанционного управления. Реже — кнопок лицевой панели, расположенных непосредственно на самом телевизоре (см. рис. 3). В частности линейка SONY KV 29FX требует удерживать клавиши PROG + и PROG - при включении питания. Пульт дистанционного управления при этом начисто игнорируется, что делает эти модели неподвластными взлому. К радости хакеров, таких телевизоров относительно немного. Производители все еще не осознали угрозу, исходящую от инженерного меню, а потому не предпринимают никаких шагов для его защиты.

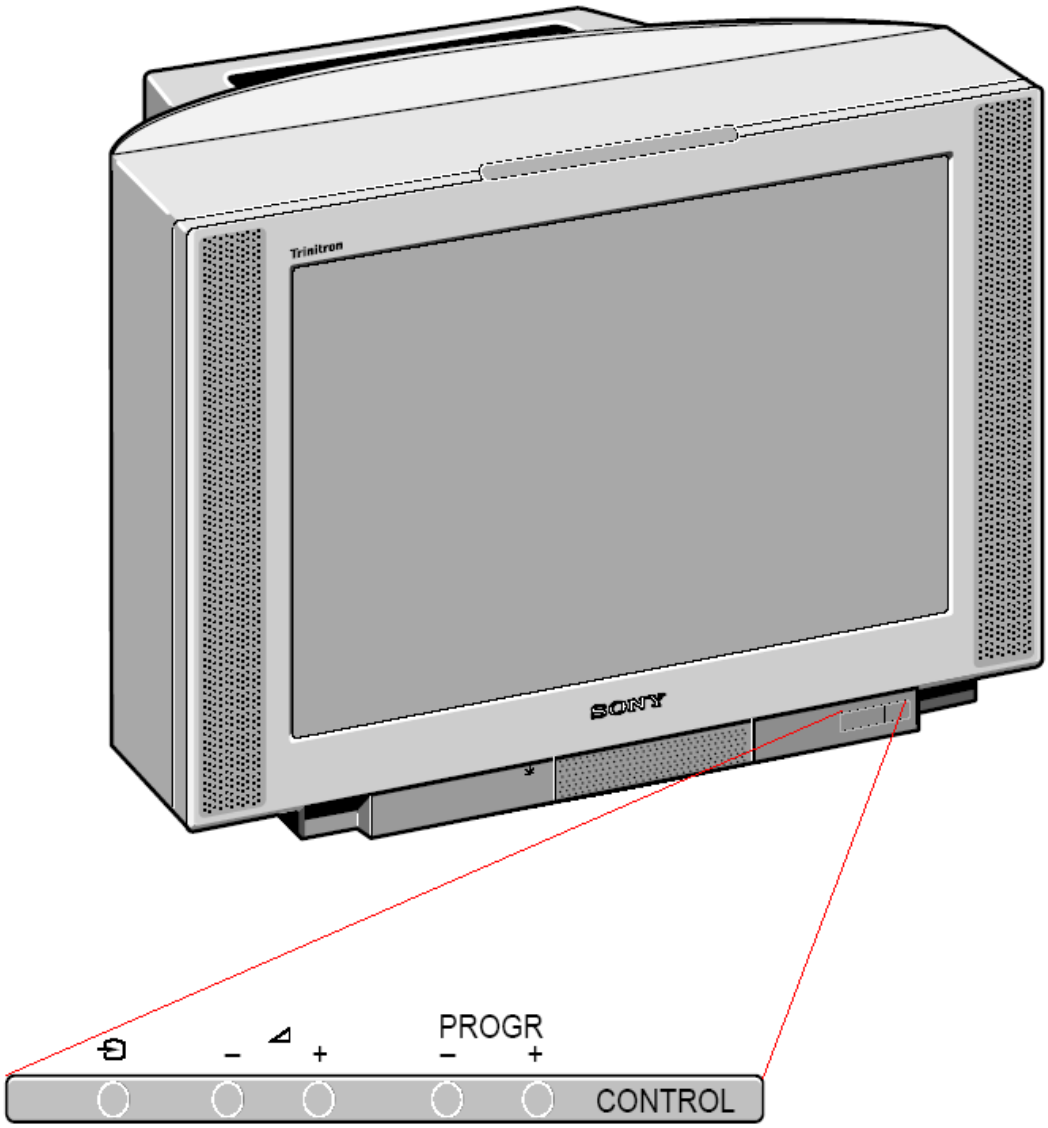

Рисунок 3 вход в инженерное меню телевизора SONY KV 29FX осуществляется только локальным способом — через кнопки, расположенные на лицевой панели

В исключительных случаях требуется специальный пульт управления, который можно приобрести на радио рынке (см. рис. 4), или собрать на основе уже готовых пультов по схемам, найденным в сети (например, monitor.espec.ws/section1/topic60458.html), ведь по сути дела, все сводится к изучению определенной последовательности инфракрасных импульсов, которую очень легко запрограммировать на любом процессоре (хоть на том же ПК с ИК-адаптером). Главное — знать протоколы передачи данных, кратно рассмотренные в одноименной врезке.

Рисунок 4 специализированные пульты управления, предоставляющие доступ к инженерному меню

Некоторые модели телевизоров фирмы SHARP позволяют добраться до инженерного меню только через непосредственное вмешательство в цепь управления процессором (в частности, модель 14/21 JN1 требует подачи 5 Вольт на 37'ую лапу микроконтроллера). Однако, это уже экзотика, достойная лишь упоминания, но не более того. Основное внимание мы сосредоточим на телевизорах, вызывающих инженерное меню определенной комбинаций клавиш со штатного пульта управления.

Комбинация эта у каждого семейства телевизоров своя. Она отсутствует в руководстве пользователя, но с той или иной степенью подробности описывается в технической документации, распространяемой в узком кругу сервисных центров или аттестованных телемастеров. Никакого секрета она не представляет и чаще всего отдается без всякого NDA

(*Non - Disclosure Agreement* – отдаленный аналог советской "подписке о неразглашении", не путать с National Drug Agency, сформированным в Риме 1 января 1999), а потому на многих радиолюбительских сайтах можно найти целую коллекцию подобных комбинаций, крупнейшим из которых, является www.telemaster.ru (см. рис.5).

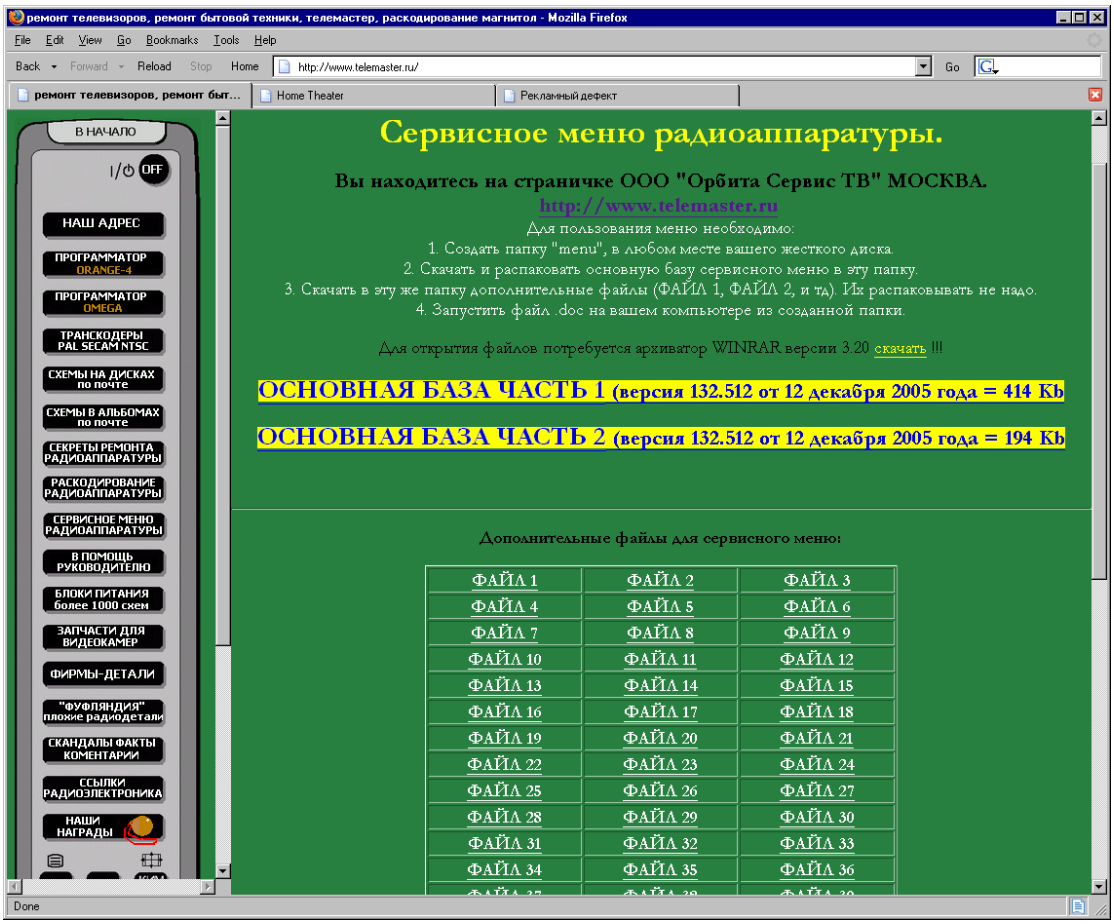

Рисунок 5 коллекция описаний комбинаций клавиш для входа в инженерное меню разной аппаратуры

Много полезной информации публикует и журнал "Ремонт электронной техники" (http://www.elcp.ru/), но, к сожалению, в отрытый доступ выложены только журналы, опубликованные до середины 2003 года (см. рис. 6), а за остальные приходится платить. Впрочем, телевизоры в плане обновления (upgrade) намного более консервативны чем компьютеры и большинство населения довольствуется "ящиками" пяти - десятилетней давности. К счастью, инженерное меню подробно описано в четвертом и пятом номерах РЭТ'а за 2001 год, которые на сайте все-таки есть.

Рисунок 6 журнал "Ремонт электронной техники" содержит уйму полезной информации для хардверных хакеров

На худой конец, можно обратиться за помощью на какой-нибудь ремонтный форум, например, http://monitor.espec.ws/section1/ (см. рис. 7). С определенной степенью вероятности там помогут.

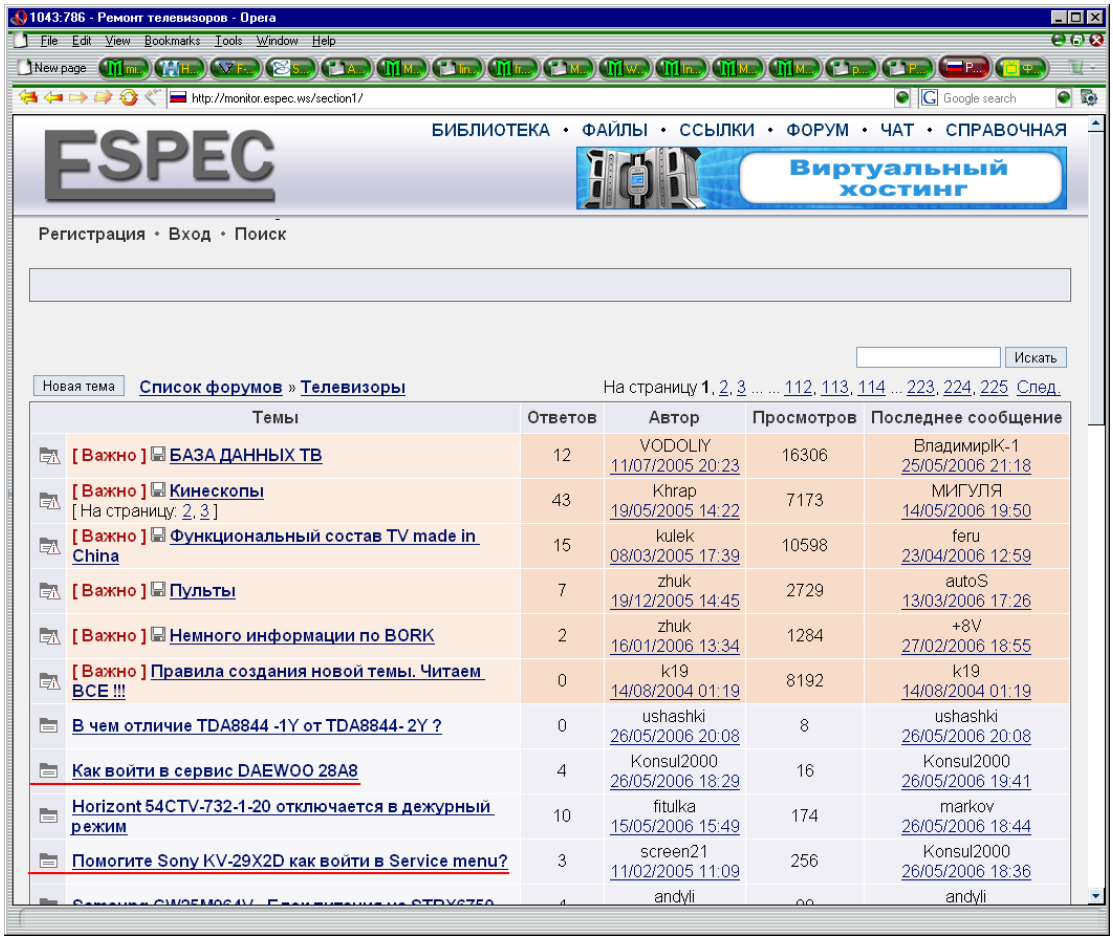

Рисунок 7 форум мастеров ESPEC, на котором можно быстро получить ответ на интересующий вопрос

Наконец, можно приобрести весьма недурственную книжку "**Home Theater Hacks**" от O'Reilly (см. рис. 8) — там взлому инженерных меню посвящен целый раздел, правда, перечня конкретных комбинаций клавиш для каждой модели телевизора, увы, нет.

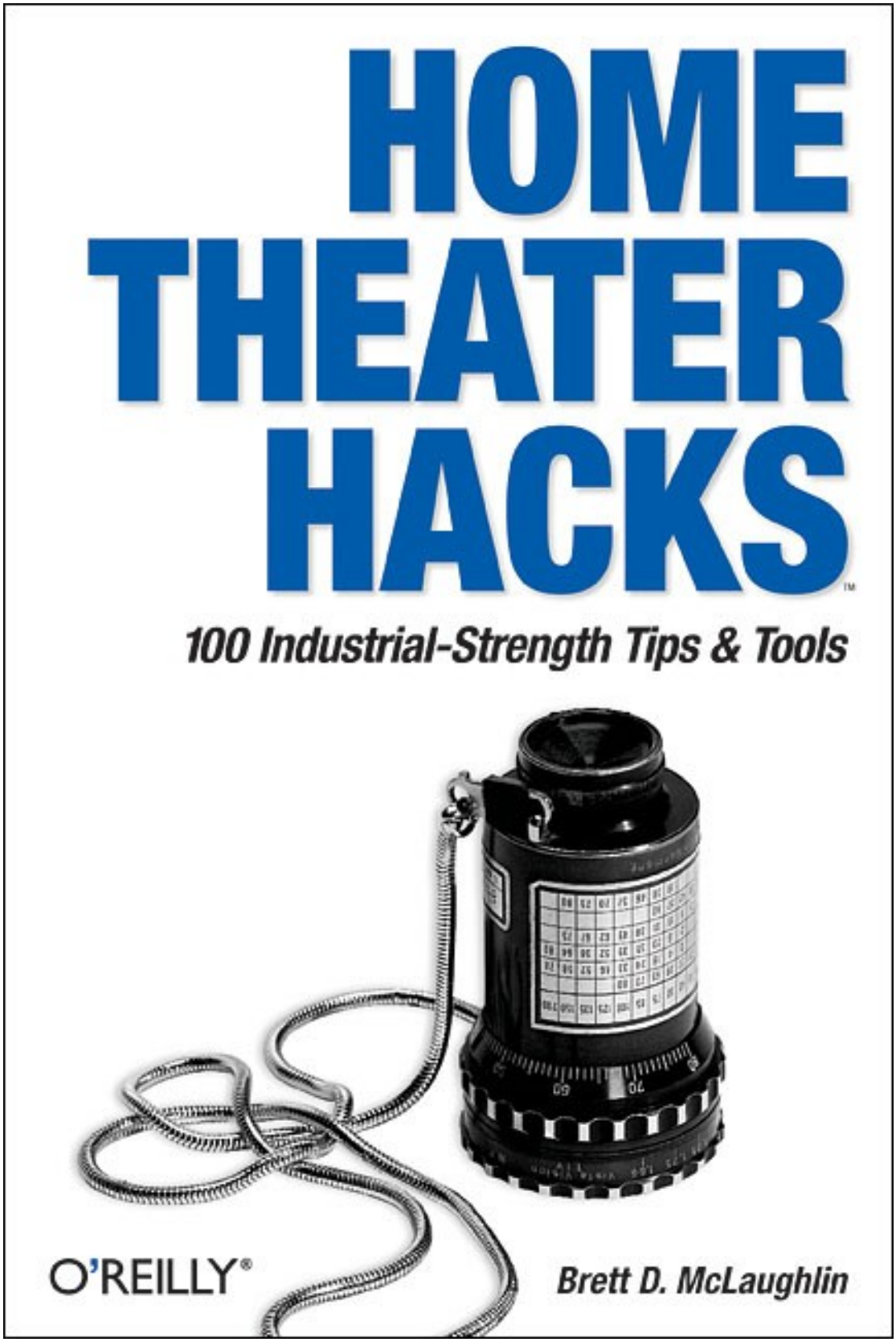

Рисунок 8 "как превратить утюг в космический корабль, оставшись при этом на свободе"

В частности, для большинства телевизоров фирмы SONY вызов инженерного меню осуществляется так: в режиме Standby (когда горит красный светодиод на лицевой панели), нажимается следующая последовательность клавиш на пульте управления (см. рис. 9).

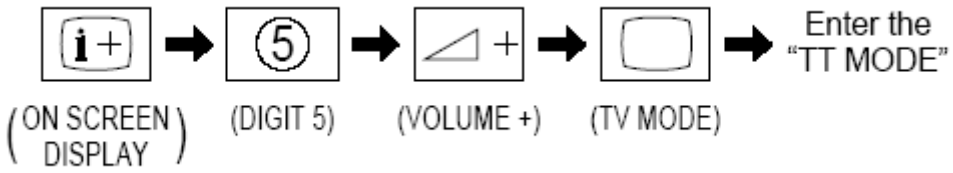

Рисунок 9 вызов инженерного меню на телевизорах SONY (не для всех моделей!)

Если все ОК, телевизор немедленно переключается в так называемый ТТ-режим (tempo time), легко опознаваемый по надписи "ТТ--" в верхнем правой углу экрана и статусной информацией ниже него.

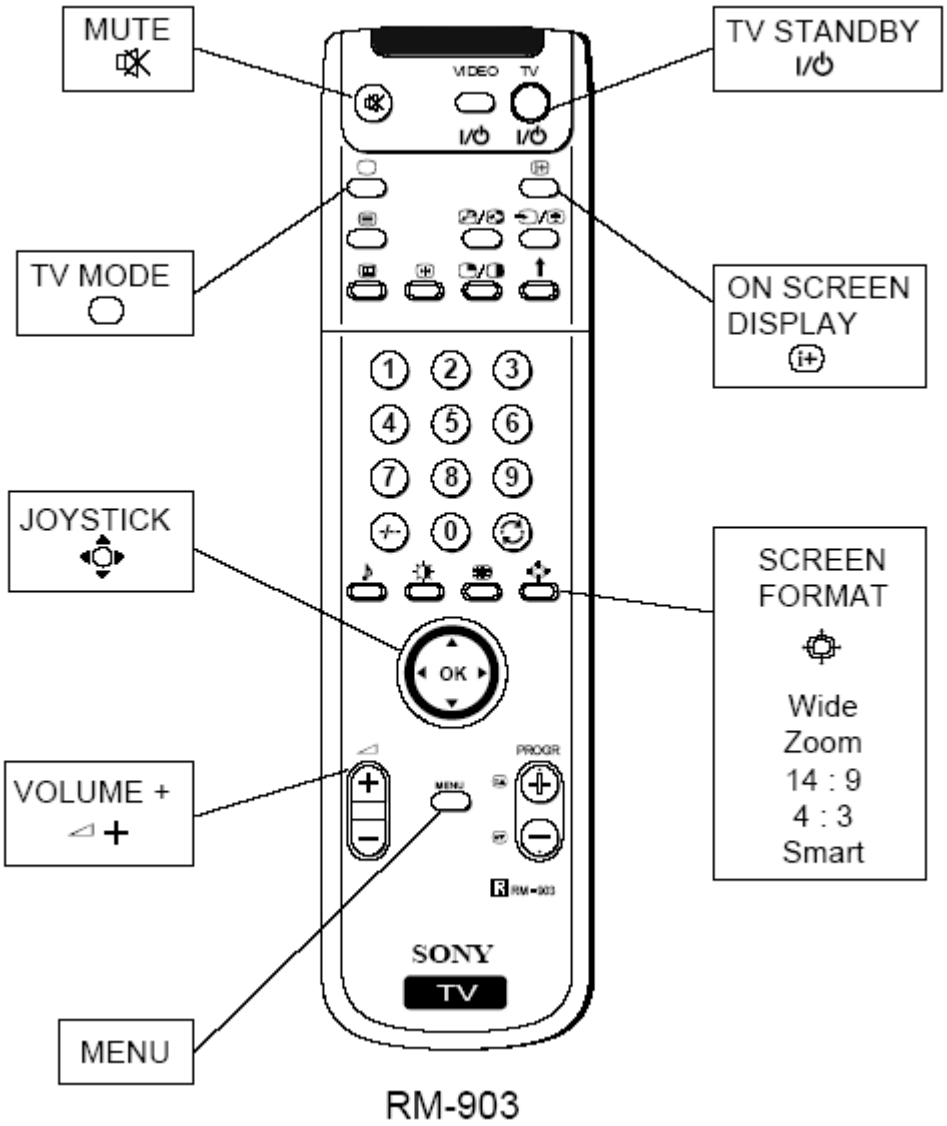

Рисунок 10 условные обозначения клавиш пульта дистанционного управления телевизорами SONY

Переход в сервисное меню из ТТ-mode осуществляется двукратным нажатием клавиши <menu> на пульте управления до появления следующей картинки (см. рис. 11). Что делать дальше — сообразить нетрудно. Перемещаясь по пунктам меню "джойстиком" (кнопка <joystick>) подводим курсор к нужному пункту и нажимаем <OK>. Выход из инженерного меню обычно происходит по нажатию Standby на пульте управления (с сохранением всех измененных параметров) или путем выдергивая телевизора из розетки (измененные параметры

при этом не сохраняются). Кстати говоря, последнюю операцию можно реализовать и удаленно, вооружившись пневматической винтовкой и перебив силовой шнур (шутка!) или обесточив квартиру рубильником на щитке (щиток — это уже не шутка! щиток — это очень серьезно, за него могут и морду набить!).

Любопытный нюанс — большинство телевизоров имеет специальный счетчик входов в инженерное меню и если в сервисном центре увидят, что здесь кто-то уже побывал, то в гарантийном ремонте могут запросто отказать, выставив клиента пинками за дверь, впрочем, это не совсем законно и потому может быть обжаловано в суде, только вряд ли что из этого получится (высказывание "а судьи кто?" спустя века все еще остается в силе).

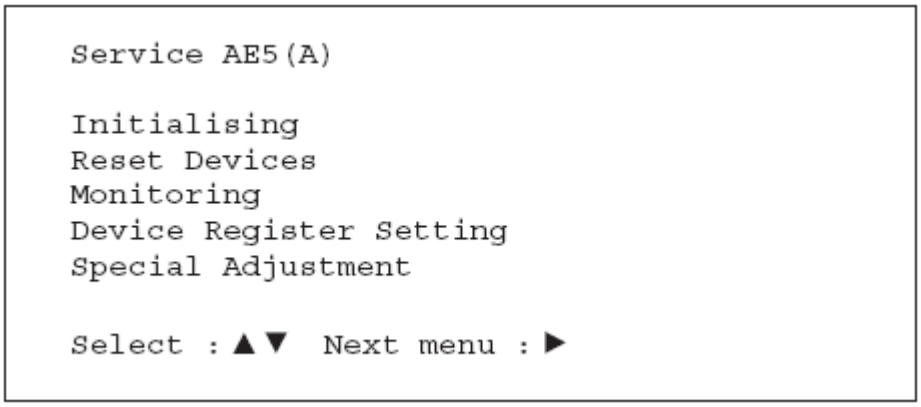

Рисунок 11 схематичный вид инженерного меню телевизоров SONY

Основная сложность заключается в том, что экран телевизора-жертвы зачастую недоступен охотнику и все действия приходится выполнять "вслепую", а для этого необходимо заранее потренироваться на телевизоре схожей или идентичной модели. Названия большинства пунктов говорят сами за себя и при желании качество изображения можно не только ухудшить, но и улучшить! Особенно это касается бракованных партий, распространяемых "серыми" дилерами, или телевизоров, собранными "по лицензии" в соседнем подвале. Так устраняются геометрические искажения (см. рис. 12), уходит ненормальная краснота лиц и многие другие дефекты, объясняющиеся небрежной настройкой, котора в условиях подпольной сборки становится слишком обременительной.

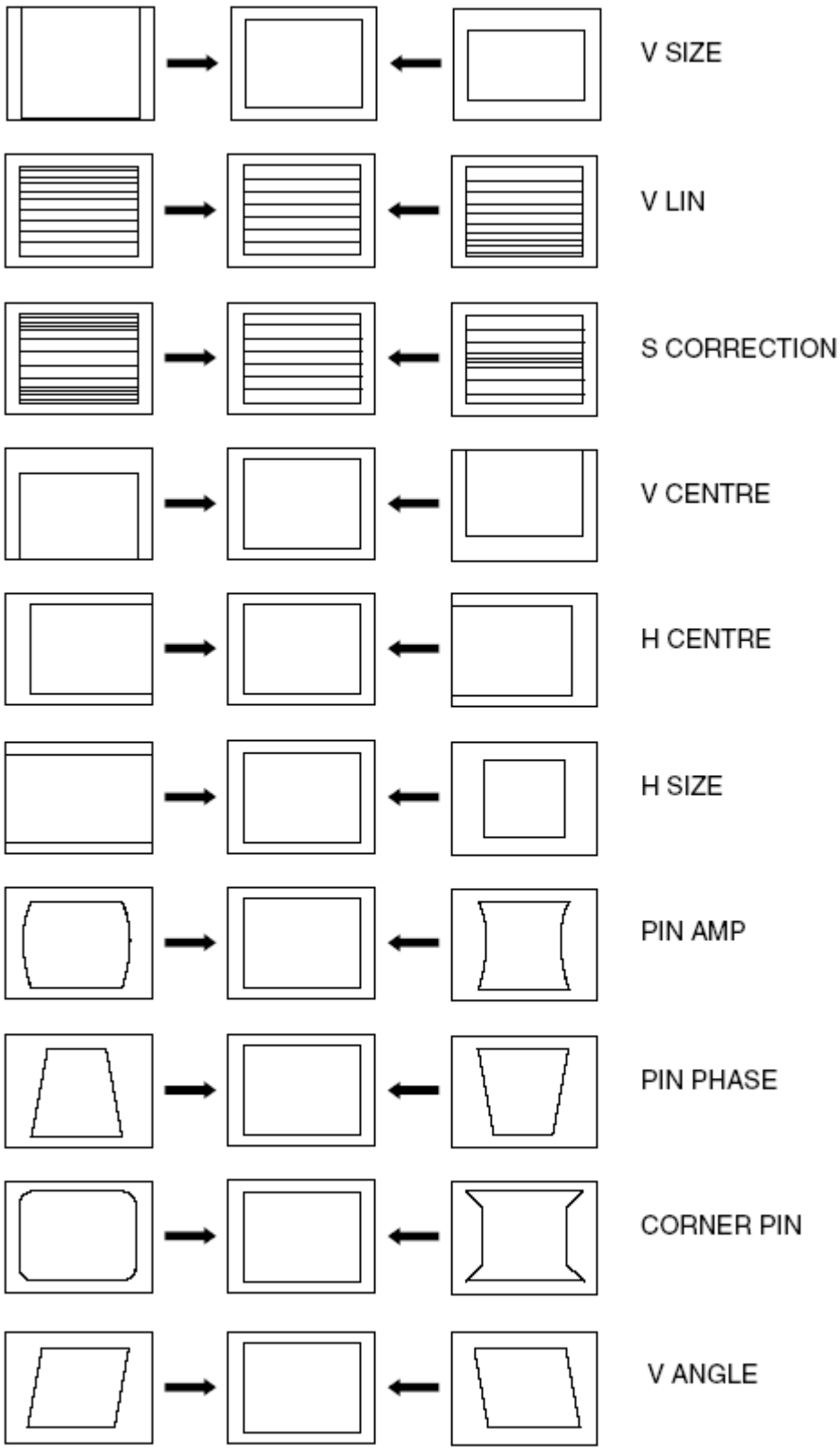

Рисунок 12 различные геометрические искажения и их типовые обозначения в инженерных меню

Находясь в сервисном меню, следует соблюдать величайшую осторожность и не в коем случае не менять тех пунктов, назначение которых доподлинно неизвестно. Одно неверное движение может запросто "убить" телевизор! Достаточно отключить развертку, чтобы

инженерное меню уже никогда не появилось на экране. Теоретически, вернуть настройки можно и "вслепую" (или поставив перед собой телевизор точно такой же модели и дублируя все нажатия на нем), но в условиях сервис центра, гораздо проще заменить микросхему энергонезависимой памяти.

Однако, это еще не самое страшное! Некоторые настройки (особенно связанные с управляющими токами и напряжениями) могут привести к физическому выходу одного или нескольких узлов из строя! (Вполне стандартная ситуация — после того как ребенок поиграл с пультом, телевизор сломался всерьез и надолго. У детей удивительная способность находить даже самые невероятные комбинации клавиш, которые никому взрослому никогда не придут в голову).

А что же на счет мониторов? Процессорные блоки у них появились уже давно, а сейчас все чаще и чаще начинают попадаться и пульты управления (очень удобно, когда монитор используется и как рабочий инструмент, и как средство для просмотра DVD). Небольшое расследование показало, что в наиболее распространенных моделях никакого инженерного меню нет, во всяком случае его нельзя вызывать ни с пульта, ни с лицевой панели, однако, прогресс не стоит на месте, электронная начинка мониторов стремительно усложняется и прошивка начинает играть далеко не последнюю роль, а там, где есть прошивка, тем есть и возможность ее обновления или настройки. Тем более, что сплошь и рядом приходится сталкиваться с ситуацией, когда одна и та же модель LCD-мониторов, выпускаемая одной и той же фирмой, в различных партиях использует матрицы от разных производителей, компенсируя разброс параметром настройкой firmware, что может осуществляется не только аппаратным путем, но и по цифровому или аналоговому интерфейсу с компьютером. Протоколы обмена пока что не разглашаются, но авторизированные сервисные центры уже имеют специальные приборы для "тонкой" настройки. Остается только перехватить сигнал и расшифровать, после чего любой хакер запросто сможет написать вирус если не выводящий монитор из строя, то приводящий изображение в непотребный вид. Прогресс, мать его…

DVD-плееры мы уже упоминали, но не стали на них акцентироваться, поскольку это тема совсем для другого разговора. Для охоты они не представляют существенного интереса, поскольку достаточно мало распространены (по сравнению с телевизорами), да и цели у хакера скорее всего будут другими (например, превратить привод в мультизональный, залить хакерскую прошивку, поддерживающую новые форматы файлов и т. д.) Выводить плееры из строя в силу их невысокой цены и отсутствия трудно-восстановимых уникальных настроек — резону нет. DVD – это не унитаз. Это хорошая штука. И ломать их не нужно.

как защититься от вандалов

Приобретая новый телевизор, заблаговременно поищите название его модели в Интернете с ключевыми словами "service menu" и посмотрите — доступен ли вызов инженерного меню с пульта дистанционного управления? За редкими исключениями, инженерное меню никогда не закрывается паролем и потому, защититься от злоумышленников программным путем никак не удастся. Лучше выбрать другой телевизор, благо на скудность ассортимента жаловаться уже не приходится.

С уже купленной аппаратурой дела обстоят намного сложнее. Но ведь не ставить же телевизор так, чтобы он не был доступен для обстрела из окон?! Далеко не каждый располагает жилплощадью, позволяющей делать такой выбор, да и к тому же обстрел может осуществляться не только прямой наводной, но и путем рикошета от стен или зеркал (убрать зеркала, на стены повесть ковры на потолок мрачные матовые обои в готическом стиле).

Самое простое и самое надежное решение — натянуть на "глазок" фотоприемника картонную трубочку длинной ~5 см, зачерненную изнутри или воспользоваться для этой цели бледной с искателя телескопа (правда, их качество зачастую оставляет желать лучшего). Конечно, легальным владельцем целиться пультом управления в телевизор будет уже сложнее, но зато это обеспечит надежную защиту от хакеров, вандалов и прочих любопытствующих.

заключение

Современная аппаратура становится все сложнее, все интеллектуальнее, все многофункциональнее, все умнее, но… вместе с тем, все уязвимее! Цифровые телевизоры позволяют обновлять свою прошивку прямо через телеэфир, а это значит, что любой хакер, вооруженный передатчиком, может внедрить в firmware своего вируса или прочую гадость.

Грядет эра тотального взлома, когда ломаться будет все, начиная от контролера внутри смывного бочка унитаза и заканчивая спутниками. Как говориться, история нас учит тому, что

ничему не учит. (c) Валентин Пашенцев. Разработчики думают о чем угодно, но только не о безопасности. И хорошо, что большинство дыр эксплуатируется хакерами-одиночками, а не профессиональным спецназом противоборствующих стран. Наказывать за невинные шалости не только глупо, но и преступно! Если подростки будут регулярно угонять с военных баз самолеты, несущие ядерные боеголовки, то судить в первую очередь следует тех, кто проектировал систему безопасности, а подростков представить к награде (хотя бы посмертно), поскольку в боевой обстановке наличие подобной дырки может очень сильно аукнуться и чем раньше удастся ее выявить — тем лучше для всех.

>>> врезка кратко о протоколах инфракрасной связи

Для самых любопытных ниже приводится краткая информация о протоколах инфракрасной связи, реализуемых в пультах дистанционного управления телетехникой. Сами протоколы реализуются готовыми микросхемами, а потому изучать принципы кодирования информации на физическом уровне никакого смысла нет. Достаточно раздобыть соответствующую микросхему и запрограммировать ее. Тем не менее, знать, что за дракон сидит в недрах кремниевого чудовища, отнюдь не бесполезно.

система IIT

Система IIT кодирует передаваемые данными путем изменения временных промежутков между короткими сериями инфракрасных импульсов (см. рис. 13). Присутствие импульса — кодирует ноль, отсутствие — единицу. Данные передаются пакетами. Каждый пакет начинается с предварительного импульса и заканчивается импульсом "стоп". Между этими двумя импульсами лежит командное слово, состоящее из 10'ти бит, 4е из которых приходится на биты адреса, а оставшиеся 6 — на биты управления. Частота генератора передатчика находится в пределах от 160 до 220 кГц.

Данный протокол реализован в микросхемах IRT1250, SAA1250 и в настоящий момент практически вышел из употребления в силу своей крайней помехонеустойчивости.

Рисунок 13 принцип кодирования информации в системе IIT

система RC-5

Для передачи информации система RC-5 использует высокочастотный несущий сигнал, модулируемый частотой полезного сигнала, равной 1/32 от частоты несущего генератора, при этом каждый бит кодируется группой, состоящей из 32 импульсов, что обеспечивает хорошую помехоустойчивость, позволяющую пульту устойчиво функционировать даже при значительной зашумленности (см. рис. 14).

Так же, как и в протоколе IIT, информация передается в виде пакетов, каждый из которых содержит:

- стартовую часть информационного бита, формируемую одним сырым битом;

- контрольную часть (действующая по принципу чет-нечет) формируется другим битом;
- "системную часть", формируемую пятью сырыми битами;
- "командную часть", формируемую шестью сырыми битами;

Система RC-5 реализована во множестве микросхем и до сих пор применяется в наше время.

Рисунок 14 принцип кодирования информации в системе RC-5

система SIEMENS

Система SIEMENS является своеобразным гибридом IIT и RC-5, объединивших их сильные черты, но не совместимым ни с одним из них. Здесь так же используется несущий сигнал, модулируемый информационным кодом и наличествуют стартовые и стоповые импульсы (см. рис. 15).

Изюминкой является механизм декодирования, "проглатывающий" пакет данных только тогда, когда переданный адрес соответствует одному из 16'ти действительных адресов, в противном случае пакет отбраковывается как дефективный. Этот нехитрый трюк позволил SIEMENS'у увеличить скорость передачи в четыре раза по сравнению с RC-5, достигнув пропускной способности до 400 кбит/сек., сохранив хорошую помехоустойчивость и снизив требования к качеству кварцевых резонаторов, используемых генераторе, что сделало протокол SIEMENS одним из самых распространенных на сегодняшний день.

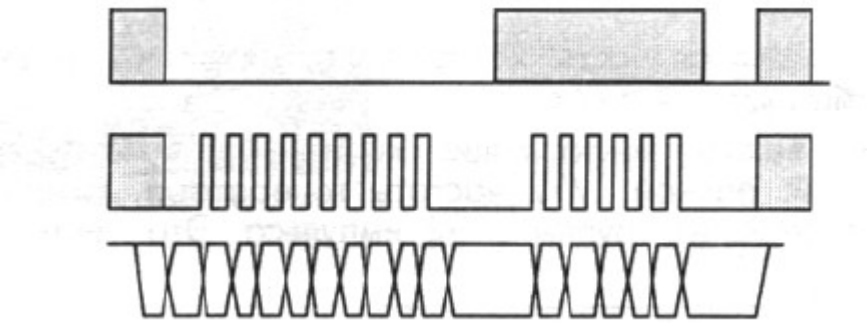

Рисунок 15 принцип кодирования информации в системе SIEMENS