А.Фантомэ
инженер, техническая защита информации.

Кишинёв
2022

ВИЗУАЛЬНЫЙ ОСМОТР ПОМЕЩЕНИЙ, ПРОВОДИМЫЙ ДЛЯ ВЫЯВЛЕНИЯ ВОЗМОЖНО ВНЕДРЁННЫХ СРЕДСТВ СЪЁМА ИНФОРМАЦИИ.

– Когда вы рассказываете, – заметил я, – всё кажется до того смехотворно простым, что я и сам без труда мог бы сообразить. А между тем в каждом конкретном случае я снова оказываюсь в полнейшем недоумении, пока вы не подскажете ход своих рассуждений. Хотя должен сказать, что глаз у меня острый.

– Совершенно верно, – ответил Холмс, вытягиваясь в кресле. – Вы смотрите, но вы не замечаете, а это большая разница.

Артур Конан Дойль, “Скандал в Богемии”.

– *Эй, Чудра! Ты почему ушёл из табора?*
– *А не те цыгане теперь пошли, не те… Коня на золото меняют!!!*
И клинок, и душу…
– *Скажи мне, Чудра, кто больше знает: дурак или мудрец?*
– *Дурак. Мудрец во всём сомневается.*
– ***Хорошо быть дураком**, Чудра!*
– *Много мудрости – много печали…*
– *Что я должен знать, если больше не увидимся?*
– *Не люби деньги – обманут, не люби женщин – обманут.*
Из всех вин самое пьянящее – это воля!
Вставай рано на рассвете и запомни, что закат приходит тогда, когда его совсем не ждёшь!
Живи, Зобар, долго и да придёт твоя смерть вовремя!

Замечательный диалог из замечательного фильма ***Эмиля Лотяну “Табор уходит в небо”***.

“***Хорошо быть дураком***” – многие, к сожалению, живут по этому принципу.

Хотя, старая английская поговорка: *“Дураку на печи лучше, чем умному в драке”* – безусловно имеет право на существование и содержит в себе глубокий смысл.

Так что **каждый должен решать сам: быть ему дураком или нет**.

Немного о “причинах всех проблем” *(моё личное мнение)*.

Каждый человек имеет своё мнение о причинах большинства проблем, которые у него возникают *(иногда разово, а иногда постоянно “по жизни”)*. Как правило, эти причины могут быть самыми различными и часто это бред: *“массовая коррупция”, “мировой заговор”, “инопланетяне среди нас” и т.д.* – чего только люди не придумают, чтобы оправдаться *(в первую очередь перед самим собой)*.

На мой взгляд, основными причинами большинства наших проблем являются **человеческая глупость** *(во многих случаях и **тупость**)* и **профессиональная некомпетентность** *(непрофессионализм)*. Наиболее ярко эти две составляющие выражены в сфере экономики (точнее сказать, в сфере *“трудовой деятельности”*) – при этом, в принципе не важно, о какой именно деятельности идёт речь: везде хватает глупцов (в том числе, среди *“заказчиков”*) и неучей *(“работников-дураков”)* среди *“исполнителей”* (естественно, что и те и другие считают себя *“умнее и круче всех”*).

Что касается деятельности, связанной с технической защитой информации в целом и с поиском средств съёма информации в частности, то *здесь человеческая глупость и непрофессионализм встречаются очень часто*.

Небольшое вступление.

Данная презентация создавалась как *“наглядное пособие”* для проведения занятий по вопросам, связанным с **технической защитой информации** в целом и с **поиском средств съёма информации** в частности.

Презентация рассчитана на “**коммерческо-частный сектор**” – на тех, кого волнует вопрос защиты своих секретов *(коммерческих и личных)*, но кто не представляет *“с чего начать”* и *“что делать”*.

Основными слушателями, для которых делалась данная презентация, были *сотрудники частных служб безопасности и личной охраны – в той или иной мере сталкивающиеся с данной проблемой и **не имеющие** какой-либо подготовки в этой области*, а так же *“отдельные граждане” (в т.ч. “заказчики”) – кого этот вопрос интересует*.

В ходе проведения занятий **ставилось две основные цели**:

первая – “стратегическая”: сформировать у слушателей представление о том, что такое **настоящая специальная проверка** помещения и объяснить им, как не попасться на “развод” со стороны *так называемых “специалистов”*;

вторая – “тактическая”: познакомить слушателей с **основными правилами** проведения визуального осмотра помещения, осуществляемого с целью выявления возможно внедрённых средств съёма информации.

Небольшое вступление.

Сразу хочу подчеркнуть, что данную презентацию нельзя рассматривать в качестве некоего “полноценного учебного пособия” *(во всяком случае, я её так не рассматриваю)*.
Я ставил перед собой задачу просто “обозначить проблему” *(как я её вижу)* и попытаться “подтолкнуть” слушателей задуматься над этой проблемой.
Можно сказать, что в презентации приведены *некоторые мои “мысли вслух”*, которые я посчитал возможным *(набрался наглости)* озвучить, исходя из своего скромного опыта работы в области ТЗИ.

Ещё раз повторю: презентация была рассчитана на людей, которые **не имеют какой-либо подготовки** в области технической защиты информации, но которые в той или иной мере сталкиваются с данной проблемой.
Я постарался максимально доступным для “неподготовленного” слушателя языком изложить элементарные вещи, связанные с проведением работ по поиску возможно установленных средств съёма информации.
Как было сказано ранее, основной целью данной презентации было **не “научить”** *(на мой взгляд, это вообще не реально в рамках “самиздата”)*, а именно **познакомить с основами** *(“базовыми” моментами)* и попытаться **сформировать** у слушателей **общее представление** по данному вопросу.

Небольшое вступление.

Структурно презентация состоит из двух “составных частей”:

- Материал первой части в основном ориентирован на “заказчиков” и предназначен тем, кто хочет пригласить “человека со стороны” для проведения проверки своего помещения.
- Материал второй части предназначен тем, кто пытается начать что-то делать по линии технической защиты информации самостоятельно – *в своей компании или для себя лично*. Вторая часть в основном ориентирована на начальников служб безопасности *(руководителей компаний)*, которые решили создать соответствующее подразделение в своей собственной компании, а так же на “непосредственных исполнителей” .

В то же время, материал обеих частей презентации достаточно “взаимосвязан”.

Внимание!

Данная презентация отражает моё личное мнение – *в котором я убеждён, в том числе исходя из личного скромного опыта работы в области ТЗИ*.

В то же время, **вполне возможно, что моё мнение – ошибочное**, а я *“торможу”*.

Поэтому всё, что я попытался “изложить” в презентации, **слушатели должны оценивать критически**, а все мои *“гениальные идеи”* обязательно должны быть проверены ими как из других источников, так и на своём собственном опыте.

Небольшое вступление.

Как было сказано ранее, данная презентация рассчитана на “коммерческо-частный сектор” – т.е. речь идёт о компаниях и частных лицах, которые начали задумываться о проблеме возможной утечки информации и пытаются начать что-то делать для защиты своих “секретов”.

При этом предполагается, что потенциальный злоумышленник так же является представителем “коммерческо-частного сектора” и может обладать соответствующими возможностями – *как материально-финансовыми, так и “административными”* – в ряде случаев “достаточно большими”, иногда – незаконными, но всё равно “ограниченными”.

Варианты, связанные с “силовыми структурами” – *когда задействуются “возможности государства”* – это совсем другое дело.

Что касается “отношений обычных граждан и государства”, то как говорится: “**Если вами заинтересовалось государство – считайте, что вам не повезло**”.

Поэтому нужно не нарушать закон и не давать повода к тому, чтобы “государство вами заинтересовалось”.

В вопросах защиты информации “*чудес*” не бывает.

Для большинства граждан вопросы технической защиты информации в целом и поиска средств съёма информации в частности представляются *“очень туманно”* и, как правило, в *“фильмово-фантастических” вариантах*:

в плане защиты – есть *“чудо-коробочка с красной кнопкой”*, которую включишь и *“никто тебя не подслушает и не увидит”*;
в плане поиска – придёт *“крутой специалист”,* у которого есть какой-то *“чудо-аппарат”*, и сразу *“всё найдёт” – даже то, чего нет*.

На самом деле **всё совсем не так** – *моё личное мнение*.

Что касается защиты, то **это целый комплекс мероприятий**, **причём основную роль в нём играют не** “**технические**”, а “**организационно-режимные**” **меры**. Естественно, что никаких *“чудо-коробочек”* **нет и быть не может**.

Что касается поисковых мероприятий, то здесь есть три важных составляющих, которые должны выполняться одновременно: **основную роль играет профессионализм** “**поисковика**”, кроме этого **важны наличие у него нужного поискового оборудования** *(в зависимости от конкретной задачи)* и обеспечение **возможности полноценно работать**.
Естественно, что никаких *“чудо-аппаратов”* тоже **не существует**.

Основной вопрос философии: “Что первично – материя или сознание?”.

Как правило, когда люди далёкие от технической защиты информации *(например, руководитель фирмы или начальник службы безопасности)* впервые “озадачиваются” этим вопросом, то в первую очередь им в голову приходит мысль: “надо срочно купить что-нибудь” – естественно, что в их представлении речь идёт о *“чудо-аппаратах, которые всё найдут”* и о *“чудо-коробочках с красной кнопкой, которые от всего защитят”*.
При этом они твёрдо убеждены, что *“мы сначала купим чудо-технику, а уже потом разберёмся, кто и как будет с ней работать”*.

Такой подход **абсолютно неправильный** – *моё личное мнение*.

Техника – “вторична” *(может и “третична”)* и с её покупкой спешить не стоит.
В первую очередь нужно определиться с человеком, который будет **реально заниматься** вопросами защиты информации,
и **обеспечить его начальную подготовку** в этой области.
Затем необходимо **правильно оценить возможные угрозы** и **составить план мероприятий, направленных на их устранение** – *как было сказано выше, основная роль отводится организационно-режимным мерам* – естественно, что это может сделать только специалист, имеющий **реальную** подготовку.

В итоге, **в ряде случаев покупка техники может вообще не понадобиться**.

Немного “молдавской статистики” *(моё личное мнение)*.

Когда речь заходит о том, кто будет заниматься вопросами технической защиты информации *(речь идёт о “коммерческо-частном секторе”)*, то в современной молдавской действительности **существует три “типовые” ситуации**:

- Об этих вопросах даже не задумываются и в компании ими вообще никто не занимается – это самый распространённый вариант (около **80%**).
- Об этих вопросах “внезапно” начинают задумываться – *обычно после просмотра руководителем очередного “шпионского” фильма или прочтения аналогичной статьи в интернете* – и срочно принимается *“гениальное”* решение о том, что *“у нас тоже кто-то должен заниматься защитой от прослушки”*. Но что конкретно нужно делать никто не знает, поэтому отдельной штатной единицы не создают, а в большинстве случаев “вешают” эти обязанности дополнительно на кого-нибудь из “личников”, “айтишников” или даже на “хозошников” – типа: *“ну ты сам разберись что и как, а дальше давай – ищи и защищай!”* – это около **5%**.
- В необходимости *“защиты от прослушки”* руководителя компании “убеждает” его знакомый, который и предлагает ему услуги *“крутого специалиста”, который “всё сделает в лучшем виде”*. После чего этот *“крутой специалист”* проводит пару *“проверок”* и предлагает в дальнейшем *“обращаться к нему – если что”*. В ряде случаев этому *“специалисту”* удаётся “развести” заказчика на покупку какой-то *“чудо-техники” – как правило, это дешёвый детектор поля или дешёвый блокиратор GSM/GPS* – это около **15%**.

Немного “молдавской статистики” *(моё личное мнение)*.

Да, в Молдове есть *(по крайней мере было)* несколько компаний, в которых к вопросу технической защиты информации относятся серьёзно, но их единицы. Так что в приведённую выше “статистику” я их даже не включал, так как это тысячные доли процента от общего числа.

Основная причина такого положения дел в области ТЗИ – **отсутствие** у большинства молдавских бизнесменов *(и не только молдавских)* **понимания необходимости такой работы** – причём **работы серьёзной**, **ежедневной** и **незаметной на первый взгляд**.

В их представлении всё опять же сводится к *“чудо-коробочкам”,* которые *“от всего защитят и всё найдут*” – естественно, что есть *“специалисты”*, которые всегда готовы предложить такую *“чудо-технику”*.

Аналогичная ситуация очень хорошо отражена у ***Юлиана Семёнова*** *в романе* ***“Бомба для председателя”***:

“Он хочет получить красивую игрушку, – понял Вабер. – Что они все понимают в науке? – подумал он, набрасывая план. – Им неинтересен поиск, они не верят в необходимость десятилетий экспериментов, прежде чем можно прийти к выводу, им важна сиюминутная отдача. И ***победит тот, кто сможет им больше наболтать математической галиматьи на уровне“доступной физики”***: сложное им, не имеющим законченного школьного образования, абсолютно непонятно”.

Немного “о кадровом вопросе” *(моё личное мнение)*.

Вопрос подготовки кадров в области технической защиты информации для работы в молдавском “коммерческо-частном секторе” является очень острым – на сегодняшний день такая подготовка в Республике отсутствует.

Если в госструктурах кадровый вопрос более-менее решается – *там другой подход и другие возможности*, то в коммерческом секторе – всё “на нуле”.

А те немногие, кто приходит из госструктур на “гражданку”, имея хоть какое-то представление о ТЗИ, сразу сталкиваются там совсем с другими реалиями и, как правило, вместо технической защиты информации занимаются металлодетекторами, охранно-пожарной сигнализацией, охранным видеонаблюдением, идут поднимать шлагбаум и т.п.

Так что фактически интерес к данной тематике проявляют только “энтузиасты”, которые *“варятся в собственном соку”* и пытаются что-то делать.

Для таких людей основным решением является самообразование – тут главное, чтобы источник информации был действительно “источником знаний”, а не *“… галиматьи на уровне “доступной физики”…” – см. предыдущий слайд*.

Примечание: естественно, что “самообразование” подразумевает наличие определённой базовой подготовки – **бесполезно пытаться что-то изучить**, **если не понимаешь азов**. Под “**базовой подготовкой**” я имею ввиду наличие у человека, начинающего изучать вопросы ТЗИ, **реальных** знаний *(образования)* в области радиотехники, связи и т.п.

Информация о сайте www.analitika.info.

В качестве одного из *“источников для самообразования”* могу скромно посоветовать посетить сайт www.analitika.info – разделы “**Форум**” и “**Информационные материалы**”. Этот сайт посвящён именно вопросам ТЗИ и на нём, *по моему скромному мнению*, компетентно обсуждаются вопросы, которые встают как перед новичками, так и перед профессионалами в этой области.

Ниже привожу несколько сообщений с форума, адресованных именно “новичкам”:

*“Основной целью форума вижу в простой форме объяснить тем, кто новичок в этой области (не является специалистом по технической защите информации – **ТЗИ**) что и как надо защищать. Ну а уж если они почувствуют потребность копать глубже – тогда в библиотеку!”*

“Одним словом, речь не идёт о “государевых делах”, а скорее направлена на тех, кто сам вынужден заботиться о защите собственных секретов.”

“Цель ресурса – обратная связь и по возможности повышение уровня знаний тех, кто начинает озадачиваться вопросами Защиты Информации.
Ведь как зачастую получается – есть подозрение в утечке, поиском в интернете находят пару статей, звонок в пару контор и дай бог консультация на часок–другой (и то вряд ли). Потом покупается некоторое количество железяк, которые через неделю после окончания параноидального обострения в лучшем случае достаются раз в полгода, чтобы показать знакомым, как клёво они находят мобилки.”

Ещё несколько сообщений с форума на сайте www.analitika.info.

“Грамотного пользователя надо подготавливать. Они не готовы ещё заниматься настолько глубоко обеспечением безопасности.
У нас ведь есть две категории: мы (ТЗИ-шники) и все остальные.
Одни понимают что и с чем едят, а другие только кино смотрели.”

“И теперь другой аспект – хорошо если организация просто берёт на работу спеца, тогда разумеется – на курсы. Это его работа. А в большинстве контор нет такого человека (к сожалению). И в лучшем случае эту задачу ставят в “нагрузку” тому, кто немного занимается с техникой. Очень часто это системные администраторы.”

“Прекрасно понимаю тех, кто не хочет заниматься глубоко ТЗИ – от своих задач по зарабатыванию денег голова пухнет, а тут еще надо вникать в вопросы, на которые на первый взгляд только деньги уходят.
Надо, чтобы система была построена так, чтобы не мешать, а помогать в работе.
И прочитав, например, наш форум – получить ответы на свои вопросы.
Ну а если захотят глубоко копать – придут и к курсам, и к найму спецов.
Там уже другой разговор. Спецам не надо объяснять как защищать помещение (хотя “спецы” разные бывают – но это тема отдельного разговора).”

Очень важна последняя фраза: “хотя спецы разные бывают …” –
“отдельный разговор” об этом см. далее.

Немного о “спецах”…

Относительно “спецов” – **у каждого своё представление о том, что значит “специалист”** *(в данном случае в области ТЗИ)*.

Как-то довелось общаться с одним индивидуумом, который заявил, что он – “профессиональный фотограф”.
На мой вопрос: “С чего ты взял, что ты “профессиональный” фотограф?” – он искренне удивился: “Как с чего? Я же за это деньги беру!”.
Потрясающий подход к вопросу “профессионализма”!!!
Я ему тогда ответил: “Тогда у нас вся страна “профессионалов”, причём “высочайшего уровня” и во всех сферах деятельности.”

По аналогии с тем *“профессиональным фотографом”* очень многие, кто имел хоть какое-то отношение к технической защите информации *(что-то слышал, что-то видел или даже “работал с приборами”)*, всерьёз считают себя *“спецом”* и *“профессионалом”*.

Ну а если у них есть свидетельство о прохождении каких-либо курсов по технической защите информации – тогда вообще *“надувают щёки”* и *“гнут пальцы”* по полной.

Немного о “спецах”…

Для таких *“специалистов” – которые “где-то что-то видели или слышали” и думают, что они реально что-то понимают и умеют* – абсолютна верна фраза из **“Двенадцати стульев”** Ильи Ильфа и Евгения Петрова:

– На всю жизнь! – прошептал Ипполит Матвеевич. – Это большая жертва.
– Жизнь! – сказал Остап. – Жертва! Что вы знаете о жизни и о жертвах? Вы думаете, что, если вас выселили из особняка, вы знаете жизнь? И если у вас реквизировали поддельную китайскую вазу, то это жертва?

В **“Двенадцати стульях”** есть один персонаж, на которого похожи очень многие *“крутые специалисты”* (кавычки!) – *Виктор Михайлович Полесов, “слесарь-интеллигент”, который считал себя знатоком всего, специалистом во всех областях и смело брался за все виды работ. Правда, в большинстве случаев он ничего никогда не доводил до конца. А если всё-таки он заканчивал начатую работу, то конечный продукт его деятельности “был очень похож на настоящий, но не работал”*.

Так и в вопросах технической защиты информации: если цель *т.н. “специалиста”* просто *“развести”* заказчика, чтобы *“срубить с него денег”* – это еще полбеды; хуже, когда такой *“деятель”* на самом деле считает себя *“специалистом”* и пытается развернуть *“бурную деятельность”* вообще не понимая, что и как надо делать.

Немного о подготовке “спецов” в Молдове.

На форуме сайта www.analitika.info есть хорошая фраза:

“Если человек начинает работать и не знает с чего начать (бывает такое), то всё же некоторое время надо бы уделить самообразованию. Интернет, в том числе и сей форум, доступная литература по ЗИ. Если денюжку начальство башляет, то курсы, желательно для начала в госконторе или в институте.
***Азы надо знать**. За руль ведь не пускают, пока на права не сдашь. Ну а дальше развиваться, насколько ума хватает.”*

Фраза абсолютно верная. Но, как было сказано ранее, она не учитывает *“молдавскую действительность”* подготовки кадров в области ТЗИ для *“коммерческо-частного сектора”* – никаких “курсов” и “институтов” по этому профилю в Республике нет и думаю, что в ближайшее время *(10 – 15 лет)* не будет.

Хотя, в то же время, в Республике действуют различные курсы по “Информационной безопасности” и в ряде молдавских ВУЗов идёт подготовка по специальности “Информационная безопасность” – другое дело, что вопросы технической защиты информации там не рассматриваются.

Так что если говорить о более-менее “полноценных” курсах по ТЗИ, то на сегодняшний день – это только за рубежом: *в частности, есть хорошие программы подготовки в Германии, Израиле, России, Румынии, США, Украине*.

Немного о подготовке “спецов”…

В то же время, нужно чётко понимать, что любые “курсы” или даже “институт” по профилю ТЗИ – это очень хорошо, но **это только** “**азы**”, которые по определению необходимо знать.
Как доказательство в математике: есть *“необходимое условие”*, но оно не является *“достаточным условием”*.

Чтобы стать **реальным** специалистом *(а тем более профессионалом)* нужны **годы реальной работы** в этой области – причём под руководством более опытных коллег, которые объясняют “нюансы” и “подводные камни”.
Ну и конечно “**опыт – сын ошибок трудных**” – естественно, в первую очередь “**своих**” ошибок – только на них можно реально научиться.

По этому поводу есть замечательная фраза у Юлиана Семёнова *(“**Бомба для председателя**”)*:

*“Я вижу, вы не хотите раскрывать все карты и это ваше право. Я могу более настойчиво просить вас показать мне всё дело, чтобы составить полное представление, но я не сделаю этого, потому что я вам многим обязан в жизни. Без ваших уроков **я бы не был юристом, я был бы обыкновенным болтуном, каких сотни в наших органах юстиции**”.*

Хорошо сказано? И таких “обыкновенных болтунов” полно везде – в том числе и в ТЗИ.

Немного о “спецах”…

Когда речь идёт о том, кто непосредственно будет заниматься вопросами ТЗИ, то с точки зрения “штатной принадлежности” возможны два варианта:

- Это фирма или физическое лицо, которые специализируются в предоставлении такого рода услуг – т.е. речь идёт о приглашении “человека со стороны” для проведения определённых работ *(разово или с определённой периодичностью)*.
- Это сотрудники самой компании, на которых возложены обязанности по защите информации – т.е. речь идёт о работниках, которые постоянно работают в компании.

В каждом из этих случаев **есть свои “нюансы”, которые нужно знать**, чтобы вас не “развели” и не “кинули” при выполнении таких работ – *в случае вызова “человека со стороны”*, и чтобы работы реально проводились, а не превратились в “имитацию бурной деятельности” – *в случае, если эти обязанности выполняет кто-то из ваших сотрудников*.

Как было сказано, техническая защита информации – это **целый комплекс мероприятий** *(в том числе и не заметных на первый взгляд)*, которые должны осуществляться постоянно.

В то же время, у большинства граждан **всё ассоциируется только с проверкой помещений** на наличие устройств съёма информации – работа, которая *“находится на виду”* и *“выглядит эффектно”*.

Некоторые рекомендации о том, как не попасть на “развод” в случае, если вы хотите пригласить для проведения специальной проверки “человека со стороны”.

– Ты снова колдуешь любовь, Джузеппе?

– Что значит любовь к женщине по сравнению с любовью к истине? А истина в том, что человек несчастен. Небо отвернулось от него. Я один на Земле делаю его счастливым: он хочет богатства – и я варю ему золото, он хочет знать будущее – и я предсказываю судьбу.

– Но ведь это обман.

*– Человек **хочет быть обманутым**, запомни это!*
***Все обманывают всех**, но делают это слишком примитивно. Я один превратил обман в высокое искусство – поэтому и стал знаменит.*

Диалог графа Калиостро и Лоренции из х/ф Григория Горина и Марка Захарова *“Формула любви”*.

Несколько слов о тех, кто *“боится, что его слушают”*.

Существуют самые разные категории лиц, которые ищут возможность *“проверить своё помещение”*, так как *“боятся, что их слушают”*.

У каждого из них свои причины: у кого-то просто *“шпиономания”* и *“паранойя”*, у кого-то *“мания величия”*, кто-то занимается “мутными” делами, кому-то это действительно нужно *(как ни странно)*.

На мой взгляд, достаточно точная характеристика некоторых “заказчиков” была дана на форуме www.radioscanner.ru:

RADIOSCANNER.RU

· Рейтинг · Объявления · Диапазоны · Таблица частот · Копилка · Радиостанции

· Начало · События · Статистика · Регистрация · Поиск · Правила · FAQ · Галерея ·

http://www.radioscanner.ru/forum/topic38663.html

Форум → Радиотехническая безопасность → Собираю статистику по характеристикам используемых СТС

Автор	Сообщение
Ушлый_тип Участник с янв 2009 Москва Сообщений: 1	Дата: 10 Июл 2009 13:43:16 # Те, кто боятся что их прослушивают: 1 Комерсанты - если проблемы с законом или уплатой налогов и они думают, что под них капают или под них действительно капают (Налоговая, ОБЭП и пр.). Просят проверить кабинет главного, зама, нач фина, бухгалтерию. - если генеральный подозревет, что под него кто то копает, зам или свои же безопасники, возможно между соучеридителями - внутренние разборки, вобщем змеиное гнездо. Просят проверить свой же кабинет, в тайне от всего коллектива. - если проподают заказчики и не могут вычислить кто их сливает конкурентам. Обычно этим грешат манагеры, но тут уже немного не та специфика - проще вычислить оперативно. 2 Госчиновники - если берут взятки и боятся быть пойманными. Просят проверить кабинет, автомобиль, дачу, особняк, баню и прочее, те места где договариваются и передают деньги. 3 Профилактика - Просят проверить ряд кабинетов - есть соотвествующий регламент, служба безопасности конторы создаёт видимость своей деятельности. - Просят проверить те кто когда то с этой темой связывался и знает что это все не придумано. Обычно тоже занимаются мутными делами. Просят подать, что нибудь для прослушивания - отправляешь на горбушку))), нередко ставят стационарные системы скрытого видеонаблюдения в своих же кабинетах и не говорят об этом...

Несколько слов *(возможно, не очень приятных)*, адресованных потенциальным “заказчикам”.

*“**Развод**”* и *“**кидалово**” (во всяком случае их попытки)* являются типовой составляющей современных *“экономических отношений”*. Сфера деятельности, связанная с предоставлением услуг по поиску устройств съёма информации, в этом плане не является исключением.

На мой взгляд, есть два основных момента, создающих благоприятные условия для возможного *“развода”* тех, кто *“хочет проверить своё помещение”*.

Во-первых, как было сказано ранее, проблема глупости *(тупости)* к сожалению является реальностью для многих потенциальных “заказчиков”. Если ты идиот *(по жизни в целом или в каких-то отдельных вопросах)* и свято веришь в существование *“чудо-коробочки с красной кнопкой”*, то это конечно печально, но тут в большинстве случаев уже ничего не поделаешь – здесь абсолютно верна классическая фраза Лёлика из “**Бриллиантовой руки**”: *“Как говорит наш дорогой Шеф: если человек идиот – то это надолго”*. Но когда из тебя делают идиота *(причём за твои же деньги)*, пытаясь тебя “развести” и “грузя” всякой *хе**ёй*, то это совсем другое дело и в этом случае каждый “заказчик” должен решать сам: *становиться ему идиотом или нет*.

Несколько слов *(возможно, не очень приятных)*, адресованных потенциальным “заказчикам”.

Во-вторых, подавляющее большинство “заказчиков” считают себя *“крутыми”* и убеждены, что их в принципе никто не сможет *“развести”* или *“кинуть”*. Естественно, что в реальности это совсем не так и те *“деятели”*, которые занимаются “разводом” клиентов, считают своих “заказчиков” просто *“тупыми комерсами, которых надо “доить” и “стричь” с них бабло”*.

По этому поводу хочется привести очень хорошую фразу одного из главных героев сериала “**Ментовские войны**”: *“Всех нас когда-нибудь губит гордыня. Когда я уверовал, что меня никто не посмеет кинуть, меня сделали как лоха”*.

Поэтому каждый потенциальный “заказчик” должен чётко понимать, что не смотря на всю его *“крутизну” (в которой он уверен)*, очень часто он рассматривается просто как *“объект для развода”* – т.е. *“лох”*.

Понятно, что “заказчик” не может *(да и не должен)* полноценно разбираться в вопросах, связанных с поиском устройств съёма информации. Но некоторые принципиальные моменты он должен представлять и понимать.

Далее будет рассказано о некоторых элементарных вещах, которые помогут потенциальным “заказчикам” ориентироваться при вызове “поисковика”.

Вы пригласили “специалиста со стороны”…

Вы “по совету друзей” или прочитав рекламу на www.999.md, решили обратиться в *“профильную фирму”* или к *“специалисту”*, предоставляющему *“услуги по поиску устройств съёма информации”*.

Как было сказано ранее, у большинства граждан (“заказчиков”) представление о такого рода деятельности “фильмово-фантастическое” – они уверены, что есть *“чудо-аппарат”*, который *“может обнаружить всё”*, а сами *“специалисты”* – это что-то среднее между Джеймсом Бондом и экстрасенсом. Причём *такие “специалисты”* при разговоре с “заказчиком” уверенно заявляют, что у них *“самое современное поисковое оборудование”* и что они *“могут обнаружить любые устройства съёма информации”*.

На самом деле в 90% случаев *(речь идёт о ситуации в Молдове)* приглашённый *“специалист”* приносит какой-нибудь *“аппарат из клоунского набора”* и гордо демонстрирует, как это *“чудо техники”* ловит “блик” от камеры мобильника на расстоянии один метр и как оно “пищит” при работе мобильного телефона. После чего *“специалист”* ходит 15 – 20 минут с умным видом по помещению, помахивая *“чудо-аппаратом”*, потом говорит классическую фразу: *“чисто”*, берёт деньги за *так называемую “работу”* и уходит.

“Заказчик” в полном восторге – *как говорится: “Блажен, кто верует”*.

Пример *“чудо-приборов”* из *“клоунского набора”*.

Что на самом деле должен делать “приглашённый специалист”.

В остальных 10% случаев у приглашённого “специалиста” может быть оборудование посерьёзнее: от различных “многофункциональных приборов” *(типа СРМ-700, “Пиранья”, “Спайдер” и т.п.)* и каких-либо средств “простого” радиомониторинга, до нелинейного локатора *(единичные случаи в Молдове)*. Увидев такую технику, заказчик вообще впадает в состояние эйфории и забывает обо всём.

Что же на самом деле должен делать “приглашённый специалист”, чтобы провести **реальную проверку** помещения, а не её “имитацию”?

Как было сказано ранее, при проведении поисковых мероприятий основную роль играет **профессионализм** того, кто их проводит, а так же **наличие** у него **необходимого поискового оборудования** и **возможности полноценно работать**.

Далее более подробно поговорим об этих трёх “составляющих”.

Немного о “профессионализме”.

Частично этот вопрос рассматривался ранее, когда речь шла о “кадровом вопросе” и о “подготовке специалистов”.

Можно добавить ещё несколько важных моментов *(моё личное мнение)*:

Настоящий специалист **в первую очередь** должен уметь правильно составить “модель нарушителя” (“модель угроз”) для проверяемого помещения – могу сказать, что большинство *так называемых “специалистов”* это словосочетание вгоняет в глубокий ступор.

Во-вторых, специалист должен чётко знать методики поиска – нужно сказать, что многие *так называемые “специалисты”* не понимают разницу между “методикой поиска” *(её они просто не знают)* и “Инструкцией по эксплуатации” на какое-либо поисковое оборудование.

В-третьих, специалист должен знать реальные возможности своего поискового оборудования по обнаружению тех или иных средств съёма информации. Это принципиальный момент, так как очень многие из тех, кто *“работает”* с поисковым оборудованием, даже не представляют “реальную картину” и без какой-либо “задней мысли” уверены в результатах своей *“проверки”*.

Некоторые примеры, касающиеся “нюансов” работы определённого оборудования, о которых не подозревают многие так называемые “специалисты” – см. далее.

Некоторые “нюансы”, которые обязан знать специалист.

Есть очень много “нюансов”, которые необходимо знать при работе с нелинейным локатором *(учитывая, что его использование обязательно при проведении спецпроверки помещения)*: в частности, **есть изделия, которые “нелинейник” в принципе “не увидит”** – например, некоторые модели экранированных диктофонов; кроме того у НЛ с автономным питанием значительно снижается мощность излучения *(“обнаружительная способность”)* при некотором разряде аккумулятора *(на двух российских и двух штатовских моделях НЛ проверено точно)*.

http://forum.analitika.info/viewtopic.php?pid=2870

15.03.2013 13:31:39 **geosfera.a**

Доброго дня!
Взял лично для себя NR-ню. Сразу говорю ограничено финансирование - плачу свои.
Все мои "коллеги" часноделы- тоже работают на себя 3-4 спеца в целом хвалили - работают и не жужжат.
Новая модификация: типа пальчиковые аккумуляторы, отсутствие сигнала их полного разряда.
Как по мне присутствует существенное снижение мощности излучения прибора при разряде аккумуляторов больше 50 процентов.
Мелочи - неудобные по форме уши, отсутствие возможности подключить сетевой блок на прямую (не знаю нужно ли...), мягкая сумка- кейс. GSM станции не взирая на подстройку частоты часто мешают.
Главное при испытаниях (гонял его, что Сидорову козу) выявил следующее:
приборы типа СТС с тонкой топологией (или единый чип)!!!!!! или при малейших намеках на металлический корпус откровенно не видит!!!!!
Сообщаю эти железки тупо не видит: Эдик, GSM няню- типа жук, блютуз передатчик на ухо, пяти вольтную мини камеру на плате управления для ноутбука,
ПЗС матрицу в полном комплекте (без корпуса и оптики), камеру в металлическом корпусе.
Отдельно проверял все это добро при режиме ВКЛ питание на железках, в т.ч. 20К- на слух, потрескивание и тишину!!!
Прошу ПЛИЗ обязательно ответить, "на корабле паника"! ВОПРОС: Что делать?? Как жить с таким чудом? Брать или нет??
Четко понимаю ответственность перед заказчиком за пропуск СТС на объекте, ведь деньги при этой работе основное, но не главное.
Да весь поисковый комплект присутствует и стандартный ответ: найдешь другим - не устраивает. ТИПА -нелинейный локатор не панацея от всех бед.
Варианты возьмите NR-2000 не предлагать или сразу дайте денег)))))))
Может посоветуете что-то другое??? за приемлемые деньги?? Ваши мысли, выводы?? Или новые методические приемы?

16.03.2013 22:43:18 **geosfera.a**

Прошу прощения, совсем забыл сказать. Все имитаторы СТС с передачей аналогового сигнала(от 200мГц до 3 ГГц), простые сотовые телефоны, родной контрольный датчик видит от 30 до 60 см.
Отклик полупроводника в наушниках от 60 до 100см. Стенку кирпича пробивает 15-20 см. спокойно.
Режим 20К слышно работает зарядки, телефоны городские и прочую электронику в режиме ВКл слышит и видит.
Но четко есть падение дальности облучения передатчика после подсаживания аккумуляторов.

19.03.2013 01:21:28 **geosfera.a**

Хочу четко сообщить:
- то, что я перечислил из оборудования прибор просто не видит и все.
- как мне кажется, вывел приблизительно- практическим путем, при разрядке аккумуляторов (не могу замерить уровень заряда) существенно даже на глаз падает дальность обнаружения электроники в т.ч. контрольного датчика. Но могу по 2 пункту ошибаться.

Некоторые “нюансы”, которые обязан знать специалист.

Реальные возможности многих “детекторов электромагнитного поля” по обнаружению радиосигналов со “сложными видами модуляции”:

Дата: 20 Дек 2013 12:52:37 # **G305e**
Участник

radioscanner.ru/forum/topic41066-5.html

готов на стоимость пираньи 032 поспорить, что она не найдёт одно серийно выпускаемое изделие даже с полуметра, работающее на частоте 423 МГц с полосой 10 МГц и так называемой "время-импульсной модуляцией". Уже не один год поставляемое тем кому положено.

Эти детекторы в современной радио-электронной обстановке в таком виде, как они сейчас делаются - "имитаторы бурной деятельности", "средство для развития паранойи у заказчика" и "приборы поиска пионерских закладок". Выбирайте название какое больше нравится.

Особенности работы с некоторыми оптическими обнаружителями видеокамер, которые необходимо знать:

Вам шашечки или ехать (Алмаз или Оптик)

http://forum.analitika.info

Пользователь: **nemo** (IP-адрес скрыт) Дата: 18, January, 2007 09:59

Попросили у меня тут обнаружитель скрытых камер. Само собой посоветовал брать Оптик 🙂. На вопрос – может лучше Алмаз – ОН ВЕДЬ ЛАЗЕРНЫЙ (!) не стал спорить.
Просто взял с собой еще и Алмаз. Заказчику зачастую видней, и нет смысла ему что-либо навязывать. Тем более оба прибора рабочие и задачу выполняют.
Объект – обычный офис. Но нюанс – хорошо освещенный. Для теста поставили две камеры. Одна – обычный цилиндр. Другая – ручка со встроенным видеопередатчиком – прикольная штука, жаль не рабочая. Китайцы молодцы.
Дал человеку сначала Алмаз. Цилиндр он нашел почти сразу. А вот ручу – нет. Т.к. театральная пауза затянулась – в течении минуты с расстояния 3 метра на площади в пару квадратных метров и зная направление он не смог найти изделие (вид камуфляжа он не знал). Дал ему Оптик – обнаружение сразу.
Вот такая вечная молодость. Посмотрели несколько человек – результат такой же. Что меня сильно расстроило?
Помимо того, что в верхней, и особенно в нижней трети объектива алмаза подсветки нет вообще, так и эфективность оказалась несколько ниже чем думал ранее.
Какие мысли по этому поводу – при поиске максимально затемнять помещение.
Я его проверял в длинном коридоре, и он не показал себя сильно слабее Оптика. Условно говоря Оптик взял там камеру с15 метров, а алмаз с 12, что вполне нормально.
Вчера же эту ручку в подвальном помещении выявили без проблемм Алмазом с 4-х метров.
Условия такие – Алмазом смотрят из освещенного кабинета в темный коридор – обнаружение сразу.
Еще нюанс – Алмазом надо работать только сверху вниз, ибо его подсветка (как и его брата близнеца Стилета) не полностью перекрывает видимую оператором область.

Немного о “необходимом поисковом оборудовании”.

Необходимо чётко понимать, что **в принципе не существует одного “универсального” прибора**, с помощью которого можно обнаружить все возможные устройства съёма информации.

Для проведения полноценной специальной проверки помещения **необходим целый набор технических средств**, каждое из которых решает свою задачу *(плюс ещё **обязателен визуальный осмотр**, но об этом отдельный разговор)*.

Если говорить о тех, кто занимается предоставлением “поисковых услуг” официально *(получив соответствующую лицензию)*, то в лицензионных условиях должен быть чётко указан минимальный набор поискового оборудования, необходимого для эффективного *(качественного)* проведения проверки.

Но, к сожалению, у нас в Республике этот момент никак не определён и в молдавских лицензионных условиях на данный вид деятельности об этом абсолютно ничего не сказано.

Поэтому в реальности получается, что формально любой, кто получил соответствующую лицензию, может совершенно спокойно *“работать”* с тем, что он сам *“считает нужным”* – точнее с тем, на что готов потратить свои деньги.

В результате большинство *“специализированных”* компаний – *не говоря уже о “свободных художниках”* – приобретают дешёвый *“клоунский набор”* и просто имитируют “бурную деятельность”.

Немного о “необходимом поисковом оборудовании”.

В итоге *“молдавская действительность”* такова, что даже если “заказчик” обратится в *“специализированную”* фирму, которая имеет официальную лицензию на предоставление услуг в области ТЗИ, то эффект от такого обращения может быть весьма сомнительным *(мягко говоря)*.

Для сравнения можно привести пример лицензирования подобных услуг в Российской Федерации – там в лицензионных условиях определены как требования к подготовке специалистов и методики проведения поиска, так и перечень обязательного оборудования, которое должно быть у лицензиата. Не буду сейчас его перечислять *(общее представление можно получить, посмотрев “**методы поиска ЗУ**” на следующем слайде)* – основной момент, который нужно отметить: для приобретения минимального набора поискового оборудования лицензиат должен “вложить” порядка **90 000 USD**.

Думаю, что **вопрос с *так называемыми “специалистами”* всем сразу стал ясен**.

Нет, конечно же и в России *(как и во всём мире)* “шаманят” будь здоров – например, история с продажей в Санкт-Петербурге баллончиков с *“чудо-спреем”*, который *“надёжно защищает оконные стёкла от прослушки по лазеру” (на самом деле это были баллончики с обычным лаком для волос)*.
Но сейчас речь идёт не о различных *“шаромыжниках”*, а о тех, кто официально занимается ТЗИ на базе полученной лицензии, и кого “заказчик” воспринимает как “лицензированного специалиста” с гарантией качества проводимых работ.

Что на самом деле должен делать и какое оборудование должен иметь в своём распоряжении “приглашённый специалист”.

Выявление внедрённых в помещения электронных закладных устройств (ЗУ) осуществляется в процессе **специальных обследований** и **специальных технических проверок** объектов информатизации и помещений.

Специальное обследование объектов информатизации и помещений проводится без применения технических средств. В ходе специального обследования поиск ЗУ осуществляется по демаскирующим признакам их внешнего вида путём визуального осмотра помещения: стен, потолков, полов, дверей, оконных рам, предметов интерьера и мебели. Особое внимание уделяется местам, куда можно быстро и скрытно установить ЗУ: под столешницами, сиденьями стульев, в различных щелях, за картинами, батареями, мебелью, шторами и т.д. Осмотру также подвергаются средства оргтехники, электрические приборы и радиоэлектронная аппаратура, средства и системы охранной и пожарной сигнализации, телефонные аппараты и т.д. При проведении специального обследования проводится тестовый "прозвон" телефонных аппаратов в целях обнаружения закладных устройств типа "телефонного уха".

Специальная техническая проверка объектов информатизации и помещений проводится с использованием технических средств и аппаратуры: индикаторов (детекторов) электромагнитного поля, радиочастотомеров, сканирующих приемников, анализаторов спектра, программно-аппаратных комплексов радиоконтроля, нелинейных локаторов, рентгеновских и рентгенотелевизионных комплексов, анализаторов проводных линий и т.д.

Эффективность поиска ЗУ во многом определяется использованием той или иной аппаратуры контроля.

К основным **методам поиска ЗУ** с использованием технических средств относятся:

- проверка помещений с использованием индикаторов электромагнитного поля;
- проверка помещений с использованием оптических средств поиска скрытых видеокамер;
- радиоконтроль (радиомониторинг) помещений;
- специальная проверка проводных линий;
- нелинейная локация;
- рентгеноскопия.

Хорев А.А. "Классификация методов и средств поиска электронных устройств перехвата информации" / "Специальная техника", № 6 2007 г.

Что значит “возможность полноценно работать”.

Бывают случаи, когда при проведении специальной проверки хозяин помещения хочет *“всё проверить, но ничего в кабинете не трогать”* – прямо как в песне из фильма “Не бойся, я с тобой!”, которую поёт бек: *“всё менять, основ не трогая”.*
Это связано с представлением многих “заказчиков” о существовании *“чудо-прибора, который сам всё найдёт”*.

Естественно, что при проведении **настоящей** проверки это не реально:
нужно всё “передвинуть”, “перевернуть”, “разобрать”, “прощупать”.
Я бы даже сказал, что при проведении **настоящей** проверки, *грубо говоря*, надо “**мудохаться**” *(в хорошем смысле этого слова)* – это нужно чётко понимать.

Другой момент связан с длительностью проведения проверки – иногда “заказчик” (опять же, уверенный в существовании *“чудо-прибора”*) считает, что для проверки достаточно полчаса *(максимум час!)* – и рассчитывает на такое время для проведения работ.

Настоящий специалист сразу скажет “заказчику”, что проверка так не делается и поставит свои условия для её проведения – или пусть обращаются к другому.

Но многие *так называемые “специалисты”* ответят “заказчику”:
“Да, без проблем! Уложимся за полчаса, ничего в кабинете не трогая!”.

Что значит “возможность полноценно работать”.

Ещё один важный момент: **для проведения полноценной проверки помещения “приглашённый специалист” должен предварительно ознакомиться с объектом проверки, чтобы знать его особенности и возможные “нюансы”**.

Если объектом проверки будет “домик в деревне”, в котором нет средств связи, электричества и вообще отсутствуют какие-либо признаки жизни в радиусе нескольких километров – это одно.

Но **в реальной ситуации** “приглашённый специалист” **должен получить информацию** о конструктивных особенностях объекта, системе вентиляции, системе электропитания, системе ОПС, системе телекоммуникаций и т.д. В ряде случаев ему нужно будет задать вопросы тем, кто непосредственно обслуживает эти системы: “айтишнику” *(связисту)*, электрику, “хозошнику” и т.д.

Иногда **без прямого участия профильных специалистов просто не обойтись**: например, без взаимодействия с системным администратором **невозможно полноценно проверить объект**, на котором функционирует своя цифровая мини-АТС, *к которой в качестве абонентских устройств подключены как “аналоговые”, так и “цифровые” аппараты (в том числе и беспроводные телефоны типа DECT)*, своя сеть VoIP, сеть Wi-Fi, локальная сеть и т.д.

Как не попасть на “развод”.

Несколько рекомендаций тем, кто хочет обратиться к “специалисту со стороны” по вопросу проведения специальной проверки:

- Независимо к кому вы обратились – в *“специализированную фирму”* или к *“свободному художнику”* – не стесняйтесь задавать вопросы, касающиеся предстоящей проверки *(даже если вы боитесь, что ваши вопросы будут выглядеть “глупо”, так как вы ничего не понимаете в этой области)*. Настоящий специалист всегда спокойно ответит на ваши вопросы и объяснит вам что и для чего он делает.
- Помните об основных составляющих, которые должны быть у “приглашённого специалиста”: профессионализм, необходимое поисковое оборудование и “возможность полноценно работать” – *причём они должны выполняться все три одновременно*.
- По завершению проверки требуйте от “приглашённого специалиста” письменного документа, в котором должно быть чётко указано, что он делал и результаты проделанной работы.
- Для проверки качества работы “приглашённого специалиста” используйте различные “имитаторы устройств съёма информации”.

Не стесняйтесь задавать вопросы “приглашённому специалисту”.

Заранее подготовьте вопросы, которые вы хотите задать по поводу предстоящей проверки: эти вопросы могут быть “простыми” (на первый взгляд), но вы должны получить на них чёткий и “мотивированный” ответ.

Основной вопрос, на который должен ответить “приглашённый специалист” – **какие средства съёма информации он может обнаружить?**

Если вам ответят что-то типа: *“мы профессионалы высокого класса”* и *“мы можем обнаружить любые подслушивающие устройства”*, то тут нужно сразу “напрячься” и вспомнить всё, что было сказано ранее про профессионализм, наличие необходимого поискового оборудования и “возможность полноценно работать” – *которые должны присутствовать одновременно*. *Может быть такие “поисковики” есть в молдавском “коммерческо-частном секторе”, но я лично не встречал и даже не слышал о них*.

Далее нужно задать следующий вопрос: *“А как вы будете искать и сколько времени вам потребуется на проведение проверки?”*.
Вот тут уже возможны различные варианты ответов, в которых “заказчику” нужно правильно “ориентироваться”.

Как не попасть на “развод” – *“универсальный чудо-прибор”*.

Если “приглашённый специалист” пришёл с каким-то *“чудо-прибором”* из *“клоунского набора” (см. фото)* и говорит вам, что с помощью него *“можно найти практически все подслушивающие устройства и скрытые видеокамеры”* – это чистый “развод” и с таким *“специалистом”* нужно сразу попрощаться.

Необходимо заметить, что это наиболее частый вариант предлагаемой *“проверки”*, с которым можно столкнуться в “молдавской действительности”.

Как не попасть на “развод” – *“детекторы электромагнитного поля”*.

Детекторы (индикаторы) электромагнитного поля позволяют оценить уровень э/м поля в данной точке *(“больше – меньше”)* и в ряде случаев могут быть полезны для поиска некоторых радиопередающих устройств, которые “активны” (излучают) в момент проверки.

Про данные изделия хорошо сказано на сайте “Лаборатории ППШ” (www.pps.ru):

“Детекторы поля – это простейшие поисковые устройства, которые необходимы для поиска радиоизлучающих подслушивающих устройств. Такой прибор нужен и начинающему специалисту (или даже совсем неспециалисту), и профессионалу. Мы предлагаем смотреть на детекторы поля как на своего рода “отвёртку”: в любом хозяйстве необходима, а если она ещё и в руках грамотного хозяина...”.

Что касается “детекторов электромагнитного поля”, то **нужно чётко понимать**: если в конце 90-х годов данные изделия *(речь идёт о “настоящих” детекторах)* ещё могли считаться одним из “основных” поисковых средств для обнаружения популярных в то время непрерывно излучающих “аналоговых” радиомикрофонов, то в настоящий момент они могут использоваться только как “вспомогательное” средство, так как в современной действительности их реальные возможности **очень ограничены** .

А ведь именно с дешёвым “детектором поля” (причём, как правило *“левым”*) до сих пор приходит в большинстве случаев *“крутой специалист”* и начинает “грузить” заказчика, что у него *“самое современное поисковое оборудование, которое обнаружит всё”* – естественно, что это чистый “развод” и с таким *“специалистом”* нужно попрощаться.

Примеры детекторов (индикаторов) электромагнитного поля.

www.das-ua.com

www.signal-t.ru

www.raksa.ru

Как не попасть на “развод” – *“сканирование радиоэфира”*.

Другая часто встречающаяся ситуация: “приглашённый специалист” на вопрос о том, какое у него поисковое оборудование, гордо заявляет, что он *“может просканировать радиоэфир и обнаружить подслушку”*.
Для “заказчика”, далёкого от вопросов защиты информации, такая фраза звучит как “бальзам на раны” – одно слово *“просканировать”* чего стоит!
В этом случае “приглашённый специалист” в качестве поискового оборудования демонстрирует поисковый или сканирующий приёмник, анализатор спектра или даже какой-нибудь простенький “комплекс радиоконтроля” – *обычно состоящий из сканирующего приёмника, подключённого к ноутбуку*.
После чего он, надев наушники, с серьёзным видом ходит по проверяемому помещению со сканером или сосредоточенно смотрит на экран монитора, на котором бегают разные непонятные для “заказчика” картинки.

Возможно, что этот “приглашённый специалист” честно “сканирует радиоэфир” *(в пределах своей подготовленности и возможностей своего оборудования)*, но есть один **очень важный момент**: сейчас не конец 90-х годов и даже не 2005 год.
Это 20 – 25 лет назад основным средством съёма информации, используемым в “коммерческо-частном секторе”, были аналоговые радиомикрофоны с непрерывным *(пока есть электропитание)* излучением – такие устройства действительно можно достаточно эффективно обнаружить “сканируя эфир”.

Как не попасть на “развод” – *“сканирование радиоэфира”*.

Сейчас ситуация, связанная со “сканированием радиоэфира”, совсем другая. В настоящий момент **подавляющее большинство радиопередающих устройств съёма информации**, используемых в “коммерческо-частном секторе”, **выполнены на базе “легальных” систем радиосвязи**: сотовая связь, Wi-Fi, Bluetooth.

Такие “радиозакладки” обладают повышенной скрытностью: **во-первых**, они работают на передачу *(т.е. “излучают в эфир”)* только в определённые промежутки времени (в 90% не совпадающие со временем проведения “разовой проверки”), а **во-вторых**, даже если “сканирование эфира” совпало по времени с работой такой “радиозакладки”, то её надо ещё “распознать” среди работающих на объекте “легальных” средств связи: мобильных телефонов, Wi-Fi и Bluetooth устройств и т.д. – *что не может быть сделано с помощью обычных средств “сканирования эфира”*.

Для **реального обнаружения** таких средств съёма информации **на объекте необходим непрерывный *(круглосуточный)* радиомониторинг** с использованием принципиально новых комплексов радиоконтроля (типа “**Кассандра**”).

Об этом есть очень хорошая статья в журнале “Защита информации. Инсайд.” / №1, 2017: **“Имитация бурной деятельности или каким не должен быть радиоконтроль в XXI веке.”** *(уже одно название статьи многое говорит даже неспециалисту в данной области)*.

Как не попасть на “развод” – *“сканирование радиоэфира”*.

Нужно чётко понимать, что “классические радиозакладки” в настоящее время активно “вытесняются” радиопередающими устройствами съёма информации, для обнаружения которых недостаточно просто “сканировать радиоэфир”. Я уже не говорю о цифровых диктофонах, проводных системах и других средствах съёма информации, которые в принципе нельзя обнаружить с помощью “сканирования эфира”.

Да, радиомониторинг является важной составляющей при поиске устройств съёма информации – *естественно, речь идёт о **настоящем радиоконтроле**, а не о его “имитации”* – но одного радиоконтроля *(даже “настоящего”)* недостаточно для проведения полноценной проверки.

Поэтому если “приглашённый специалист” уверяет вас, что он сможет *“полностью проверить помещение”* за полчаса только *“сканируя эфир”* – это “развод” и с таким *“специалистом”* нужно попрощаться.

Как сказал один человек, когда ему объяснили про такое *“сканирование эфира”*: *“Получается, что они ищут то, чего нет и не должно быть в кабинете?”* – по большому счёту он прав.

Примеры оборудования, используемого для “сканирования эфира”.

www.aor.com

www.reiusa.net

www.nera-s.com

Немного об обнаружении т.н. “GSM-передатчиков”.

Как было сказано ранее, в настоящее время **подавляющее большинство радиопередающих устройств съёма информации**, используемых злоумышленниками в “коммерческо-частном секторе”, **выполнены на базе “легальных” систем радиосвязи** – в частности, на базе сотовой связи.

Наибольшее распространение получили т.н. “**GSM-передатчики**”.

Как было отмечено, такие изделия включаются “на передачу” дистанционно только в определённые промежутки времени, которые в большинстве случаев не совпадают со временем проведения “разовой проверки”.

Поэтому для того, чтобы “засечь” факт работы GSM-передатчика “на излучение”, нужно или осуществлять непрерывный круглосуточный радиомониторинг в проверяемом помещении, или “принудительно” активировать GSM-передатчик.

Конечно, во многих случаях “заносной” GSM-передатчик может быть обнаружен с помощью нелинейного локатора или при визуальном осмотре помещения.

Но при “глубоком камуфляже” *(например, в “штатную” электронику)* имеет смысл сперва “поймать” факт работы передатчика, чтобы убедиться, что он реально есть “где-то в проверяемом помещении”, а потом уже искать его “до победного конца”.

Примечание: *под условным наименованием “GSM-передатчик” здесь понимаются все радиопередающие устройства съёма информации, работающие на базе сотовой связи, независимо от конкретного стандарта: GSM, 3G, 4G, CDMA-2000 и т.д.*

Немного об обнаружении т.н. “GSM-передатчиков”.

Для “**кратковременной активизации**” GSM-передатчика, находящегося в “ждущем режиме”, можно использовать процедуру “перерегистрации в сети”. Этот вопрос подробно обсуждался на форуме www.analitika.info ещё в 2006 г.

Для “принудительной” перерегистрации GSM-передатчика в сети необходимо гарантированно “заглушить” сигнал сотовой связи в проверяемом помещении *(“разорвать” связь между GSM-передатчиком и базовой станцией)*, используя блокиратор сотовой связи.

После чего отключить блокиратор и с помощью комплекса радиомониторинга, анализатора спектра или хорошего детектора электромагнитного поля зафиксировать момент “перерегистрации GSM-передатчика в сети” – кратковременное “излучение” в соответствующем диапазоне частот.

Конечно, здесь есть много технических и организационных “нюансов”, которые должен знать “приглашённый специалист”, проводящий поисковые работы: период “перерегистрации” задаётся оператором сотовой связи и достигает иногда десятков минут, в течении которых нужно “сидеть и ждать сигнала”; есть вероятность “поймать” ложный сигнал от легальных мобильных телефонов, находящихся в соседних помещениях, которые тоже попали в зону работы блокиратора сотовой связи и теперь “ищут сеть”, а также ещё целый ряд моментов – в общем, “не всё так просто”.

Немного об обнаружении т.н. “GSM-передатчиков”.

Нужно понимать, что при “перерегистрации” GSM-передатчика *(при “кратковременной активизации”)* нельзя его локализовать *(т.е. обнаружить само изделие)*, так как длительность “передачи” очень короткая.

В данном случае можно только с определённой вероятностью определить *есть* или *нет* данное изделие в проверяемом помещении.

Для дальнейшей локализации *(непосредственного обнаружения)* GSM-передатчика необходимо провести его поиск с помощью нелинейного локатора и визуального осмотра помещения.

www.signal-t.ru

Немного об обнаружении т.н. “GSM-передатчиков”.

Кроме “кратковременной активизации” GSM-передатчика, находящегося в “ждущем режиме”, возможна и его “**длительная принудительная активация**”. Для этого используются так называемые “ложные базовые станции” или “имитаторы базовой станции” (ИБС).

Данные изделия позволяют “подменить” базовую станцию сотовой связи и “взять на себя” управление абонентскими устройствами, находящимися в зоне действия такого комплекса. После этого все GSM-устройства могут быть принудительно переведены в “режим передачи” (“излучения”) на длительное время, в течении которого их можно обнаружить и локализовать – например, с помощью хорошего детектора поля.

Такие комплексы очень эффективны для поиска GSM-передатчиков, но тут тоже есть определённые “нюансы” *(причём принципиальные)*:

- Данные изделия фактически являются т.н. “кэтчерами” и находятся “на грани” СТС.
- Каждый “кэтчер” работает только со “своим” стандартом связи. Наиболее распространены ИБС стандарта GSM (2G), а более “высокие” стандарты (3G и 4G) обычно “подгоняются” под 2G путём “подавления” соответствующих диапазонов частот и “перевода” мультистандартных закладных устройств в режим “чистого” GSM. Но многие закладные устройства, работающие в стандартах 3G или 4G *(не говоря уже про CDMA-2000 и т.д.)*, в принципе не могут быть “переведены” в 2G – в них “жёстко” установлен только один стандарт. Хотя на данный момент в “коммерческо-частном секторе” злоумышленниками наиболее часто используются “закладки”, работающие именно в стандарте GSM (2G), но идёт “стабильный рост” и других стандартов.
- Цена комплекса составляет от **30 000** USD – это только для одного стандарта сотовой связи. Соответственно для “полноценного набора” стандартов цена будет пропорционально расти.

Пример имитатора базовой станции GSM *(модель “ИБС-2G”)*.

www.tezasys.ru

Назначение

Имитатор предназначен для обнаружения, идентификации и местоопределения электронных устройств негласного получения информации, использующих для передачи информации каналы сотовой связи.

Технические характеристики

Наименование	Значение	Примечание
Возможности оборудования по активному поиску устройств сотовой связи	Имитатор выполняет роль ложной базовой станции GSM 900/1800 МГц	Для принудительного перевода мультистандартных закладных устройств в режим GSM рекомендуется осуществлять подавление в диапазонах 3G/4G с помощью ПАК «Саламандра/Саламандра 2»
Габаритные размеры радиомодуля (кейса)	365x286x117	ШхВхГ, мм, не более
Вес радиомодуля (кейса)	4	кг, не более
Мощность радиопередатчика GSM	2	Вт, не более

Краткое описание

Имитатор «ИБС-2G» управляется и настраивается при помощи ПЭВМ (ноутбук).
Оператору предоставлена возможность развернуть на месте проведения работ ложную базовую станцию GSM 900/1800.
При этом произвольно настраиваемыми являются следующие параметры БС:

- имя оператора (код страны MCC, код сотовой сети MNC)
- номер канала (CH, частота)
- номер базовой станции (Cell ID)
- код локальной зоны LAC (Local Area Code)

Принцип работы

Имитатор принудительно в автоматическом режиме переводит находящиеся в помещении устройства сотовой связи стандарта GSM под свое управление. Затем становятся доступными следующие функции:

- определение IMEI/IMSI обнаруженных устройств;
- отправка произвольного SMS;
- перевод GSM-устройства в активный режим (режим передачи) на продолжительное время.

При удержании устройства в активном режиме с максимальной излучаемой мощностью оператор обнаруживает GSM-закладку в помещении с помощью узкополосного индикатора поля (приобретается отдельно).

Круглосуточный радиоконтроль – реальная необходимость при проверке серьёзных объектов.

Как было ранее сказано, в настоящее время большинство радиопередающих средств съёма информации не работают “на передачу” постоянно – поэтому вероятность “поймать” их излучение в ходе “разовой” проверки крайне мала. Для обнаружения факта работы таких устройств **необходимо осуществлять непрерывный *(круглосуточный)* радиомониторинг** проверяемого помещения. Естественно, что под “непрерывным радиомониторингом” понимается **не просто** круглосуточная “работа” сканирующего приёмника или анализатора спектра, а речь идёт об использовании высокоскоростных аппаратно-программных комплексов радиоконтроля, позволяющих сохранять все результаты измерений параметров радиоизлучений для их последующего детального анализа. Такие комплексы должны иметь высококачественный приёмный тракт и мощное программное обеспечение, необходимые для обнаружения и идентификации не только “простых” радиопередатчиков, но и устройств, использующих для передачи информации широкополосные, шумоподобные и другие “сложные” сигналы, а так же “легальные” каналы связи типа Bluetooth, Wi-Fi, DECT, CDMA, GSM, 3G, LTE, TETRA, DMR и т.д.

Вот такая “информация к размышлению”: кто из “заказчиков” может похвастаться тем, что при проверке у него был организован **настоящий** круглосуточный радиоконтроль?

Примеры комплексов радиоконтроля “Кассандра”.

По совокупности своих технических возможностей комплексы серии “**Кассандра**” на данный момент практически на имеют аналогов *(как минимум, в “открытой” продаже)*. Используемые в них уникальные аппаратно-программные решения позволяют выполнять самые сложные задачи радиоконтроля – в том числе, связанные с обнаружением несанкционированных радиоизлучений в проверяемых помещениях.

Подробная информация на сайтах www.inspectorsoft.ruПодробная информация на сайтах www.inspectorsoft.ru и www.analitika.info.

Как не попасть на “развод” – *“многофункциональные поисковые приборы”*.

Иногда “приглашённый специалист” приходит с небольшим чемоданчиком и гордо демонстрирует “многофункциональный поисковый прибор”:
СРМ-700, “Пиранью”, “Спайдер”, “ANDRE” и т.п.
При этом он рассказывает о том, что данный прибор позволяет обнаружить *“практически все типы подслушивающих устройств”* – ну или *“почти все”*.
Действительно, “многофункциональные приборы” имеют целый набор аксессуаров *(сменных антенн и зондов)*, предназначенных для обнаружения сигналов в широком диапазоне частот – как “излучаемых в эфир”, так и передаваемых по проводным линиям.
Проблема в том, что для обнаружения этих сигналов необходимо, чтобы устройства съёма информации *(в частности радиомикрофоны)* были “активны” в момент проведения проверки – а это в современных условиях крайне маловероятно *(см. предыдущие слайды про “сканирование эфира”)*.
Что касается проверки проводных линий, то это вообще “особая история” – для их полноценной проверки нужна не только хорошая подготовка “поисковика”, но и возможность подключения ко всем проводным линиям:
электросеть, телефонная линия, LAN, линии ОПС и т.д.

Как не попасть на “развод” – *“многофункциональные поисковые приборы”*.

Есть ещё целый ряд чисто “технических” моментов,
связанных с **реальными** возможностями большинства таких приборов –
но это уже “нюансы” для специалистов.

Для “заказчика” важно понимать, что *цифровые диктофоны, некоторые “проводные” системы съёма и передачи информации, не работающие на момент проверки радиомикрофоны (включая “GSM-передатчики”), а также многие другие устройства съёма информации (в том числе и “работающие” на момент проведения проверки)*
с помощью “многофункционального поискового прибора” **обнаружить нельзя**.

Да, это достаточно полезный прибор *(в умелых руках, естественно)*, но
он может использоваться только в дополнении к другим методам поиска.

Поэтому, если “приглашённый специалист” пришёл к вам с таким прибором,
с умным видом походил с ним по комнате, держа в руке выносную антенну, а
потом подключился через адаптер к электросети *(очень редкий случай)* и
на этом закончил свою *“проверку”*, сказав, что всё в порядке – то это “развод”.

Примеры “многофункциональных поисковых приборов”.

www.signal-t.ru

www.reiusa.net

Как не попасть на “развод” – *“нелинейный локатор”*.

В единичных случаях *(речь идёт о Молдове)* “приглашённый специалист” приносит с собой чемодан, в котором находится “нелинейный локатор” – один из главных поисковых приборов, необходимых для проведения специальной проверки помещения.

С помощью хорошего нелинейного локатора грамотный специалист может обнаружить различные типы устройств съёма информации, в том числе и “не работающие” на момент проведения проверки.

Какой НЛ считать “хорошим” и кого считать “грамотным специалистом” – это особый разговор.

Для “заказчика” важно понимать, что **нелинейный локатор не является** “**панацеей от всех угроз**” – например, с его помощью нельзя обнаружить некоторые “экранированные” устройства съёма информации, а так же устройства съёма информации, установленные внутри “штатных” электронных приборов.

Поэтому не стоит “впадать в бурный восторг”, когда “приглашённый специалист” гордо продемонстрирует вам, как он *“легко находит”* с помощью НЛ мобильный телефон в кармане куртки или пульт от телевизора под столом. Когда речь пойдёт о **реальном** поиске – там будет совсем другая ситуация.

Как не попасть на “развод” – *“нелинейный локатор”*.

В качестве типового примера “развода” можно привести фрагмент из статьи *“**У стульев тоже бывают уши**”* – в ней интервью с одним специалистом по обнаружению устройств съёма информации:

“Мы приехали на проверку. Проводим её по всем правилам, не оставляя “белых пятен”. Работаем 2,5 часа. А заказчик ходит вокруг и говорит: “Что-то вы плохо работаете!”. Мы отвечаем, что всё идёт по плану в соответствии с методиками поиска. А он в ответ рассказывает, что приезжал к нему парень, походил полчаса с “метёлкой” (нелинейный локатор), заработал тысячу долларов и уехал, и ставит его в пример”.

Поэтому, если “приглашённый специалист” пришёл к вам с нелинейным локатором и провёл за полчаса *“проверку”*, используя только этот прибор и ничего больше не делая, то это “развод” – *пусть и более дорогой (т.к. НЛ стоит прилично)*.

Отдельный разговор по поводу подготовки “поисковиков”:
при работе с НЛ есть очень много “нюансов” и “тонкостей”, которые многие *“крутые специалисты”* не знают и не понимают.
В результате они *“работают”* с НЛ как с метлой или с малярным валиком – *дворники и маляры из них может были бы неплохие* –
естественно, что эффективность такой *“проверки”* будет практически нулевая.

Примеры нелинейных локаторов.

www.reiusa.net

www.detektor.ru

Как не попасть на “развод” – *“проверка проводных линий”*.

Одной из обязательных составляющих при проведении поисковых работ по обнаружению средств съёма информации является проверка **всех** проводных линий, проходящих через помещение: электросеть, кабели телефонной и локальной сети, линии охранно-пожарной сигнализации и т.д.

Для полноценной проверки проводных линий нужен как их визуальный осмотр *(с обязательным вскрытием кабель-каналов, в которых они проложены)*, так и исследование проводных линий с помощью специальных анализаторов – т.е. необходимо физическое подключение к каждой линии для её тестирования.

Частично функции анализатора проводных линий есть в большинстве “многофункциональных поисковых приборов”, но есть и специализированные анализаторы проводных линий – например, “**TALAN**” или “**Улан**”.

Каждый анализатор проводных линий имеет свои “нюансы” и требует особой подготовки оператора. Основной момент, который должен понимать “заказчик”: для реальной проверки необходимо гальваническое (контактное) подключение анализатора к каждой линии, проходящей через помещение.

Поэтому если *“специалист”* подключился “Пираньей” на пару минут только к одной электрической розетке, а к остальным кабелям *(телефон, LAN, ОПС)* вообще не прикасался – то это “развод”.

Примеры анализаторов проводных линий.

www.reiusa.net

www.novocom.ru

Как не попасть на “развод” – *“проверка телекоммуникационного оборудования”*.

При проведении поисковых работ по обнаружению средств съёма информации **обязательно должно быть проверено** всё находящееся в помещении телекоммуникационное оборудование и средства оргтехники: *телефонные и факсимильные аппараты, персональные компьютеры, принтеры, “рутера” и т.д*.
А при проведении **комплексной** специальной проверки объекта **необходимо проверить** не только “абонентское” оборудование, но и мини-АТС *(если она есть)*.

Необходимо чётко понимать, что в телекоммуникационное оборудование могут быть внедрены как средства съёма информации, передаваемой по каналам связи, так и средства съёма речевой и видовой информации, циркулирующей в помещении – подробнее об этих угрозах рассказано в презентациях *“Технические каналы утечки информации, передаваемой по каналам связи”*, *“Технические каналы утечки акустической информации”* и *“Способы и средства обнаружения скрытых видеокамер”*.

При этом нужно помнить, что установленные в телекоммуникационное оборудование “закладки” могут быть чисто **аппаратными** *(различные варианты “классических” ЗУ)*, **аппаратно-программными** и чисто **программными** – например, изменение программных настроек “цифровых” мини-АТС, использование т.н. “Spy Phones” *(“телефонов-шпионов”)* или внедрение “программы-шпиона” в персональный компьютер *(“планшет”, смартфон)*.

Как не попасть на “развод” – *“проверка телекоммуникационного оборудования”*.

Соответственно, при проверке телекоммуникационного оборудования необходимо использовать различные методы поиска закладных устройств.

Если “аппаратные закладки” могут быть обнаружены при визуальном осмотре оборудования *(более подробно об этом будет рассказано далее)*,

то для обнаружения “программных закладок” необходим анализ программных настроек телекоммуникационного оборудования и проверка данного оборудования с помощью специальных программ – по аналогии с проверкой “антивирусными” программами.

Поэтому, если “приглашённый специалист” просто “поводил” возле телефонного аппарата и компьютера индикатором поля (без их разборки и тщательного визуального осмотра), а к остальному оборудованию вообще не подходил (типа: *“ну стоит себе рутер и ладно”*) – это чистый “развод”.

Ещё один важный момент, который должен чётко понимать “заказчик”: при грамотной проверке телекоммуникационного оборудования можно обнаружить внедрённые в него “закладки” и некоторые средства съёма информации, подключённые к кабельным линиям.

Но при этом в принципе **нельзя** ответить на вопрос, который часто задают некоторые “заказчики”: “**Прослушивается мой телефон или нет**?”. Поэтому если вы услышите от “*специалиста*” что-нибудь типа: *“я проверил ваш телефон – он не прослушивается”*, то такое *“серьёзное заявление”* это даже не “развод” – это просто бред.

Как не попасть на “развод” – *“поиск скрытых видеокамер”*.

Иногда “приглашённый специалист” может прямо заявить, что он занимается только поиском скрытых видеокамер – как правило, это связано с его “экипировкой” (когда в распоряжении “специалиста” имеется только обнаружитель видеокамер).

В принципе, если “заказчика” волнует только угроза скрытой видеосъёмки, то к такому “специалисту” можно обратиться.

Основная проблема заключается в том, какой именно обнаружитель видеокамер имеется у “приглашённого специалиста”, и на сколько грамотно он умеет с ним работать.

Если у него какая-то *“безделушка со встроенным красным стёклышком”* из *“клоунского набора”* (примеры подобных *“чудо-приборов”* были ранее), то это “развод” и с таким *“специалистом”* нужно сразу попрощаться.

Если же у “приглашённого специалиста” имеется настоящий оптический обнаружитель скрытых видеокамер (например, “**Оптик-2**” или “**Чистильщик**”), то всё зависит от его профессионализма – грамотный “поисковик” с помощью такого прибора сможет обнаружить практически любые скрытые видеокамеры, используемые “злоумышленниками” в “коммерческо-частном секторе”.

Примечание: *более подробно вопросы поиска видеокамер рассматриваются в презентации “Способы и средства обнаружения скрытых видеокамер”*.

Примеры профессиональных обнаружителей видеокамер, работающих по принципу “эффекта световозвращения”.

www.anti-systems.ru

Как не попасть на “развод” – *“тепловизор”*.

Некоторые “приходящие специалисты” приносят с собой т.н. “тепловизор” и используют его в качестве *“основного”* поискового прибора при проведении проверки помещения.

В молдавском “коммерческо-частном секторе” используются исключительно “бюджетные” тепловизоры *(стоимостью до 1500 USD)*, предназначенные для контроля качества строительно-монтажных работ: обнаружение “тепловых утечек” из-за плохой термоизоляции зданий, поиск “греющейся” электропроводки и т.п.

Нужно чётко понимать, что данные приборы по своему “основному” функциональному назначению не предназначены для поиска средств съёма информации и могут использоваться для этой цели с большими “условностями”.
Например, такой тепловизор позволяет с достаточно высокой эффективностью обнаружить работающие на момент проведения проверки видеокамеры различных типов *(т.е. те видеокамеры, у которых в момент проведения проверки “греется матрица”)*.
В то же время, эффективность такого тепловизора будет практически “нулевой”, если камера в момент проведения проверки будет выключена.

Для “заказчика” важно понимать, что практически все средства съёма информации, не работающие *(не “греющиеся”)* на момент проведения проверки, с помощью “бюджетного” тепловизора **обнаружить нельзя** и его “по определению” нельзя рассматривать в качестве “полноценного” поискового прибора – он может использоваться только в дополнении к другим методам поиска.

Поэтому, если “приглашённый специалист” пришёл к вам с таким прибором, с умным видом походил по комнате, направляя тепловизор по сторонам, и на этом закончил свою *“проверку”*, сказав, что всё в порядке – то это “развод”.

Пример “бюджетного” тепловизора.

Немного о средствах рентгеноскопии *(для “общего развития”)*.

При проведении специальной проверки помещения в ряде случаев может быть необходим рентгеноскопический контроль отдельных элементов, которые не могут быть “разобраны” для полноценного осмотра.

Нужно чётко понимать: рентгеноскопическому контролю могут быть подвергнуты только **отдельные элементы** – как элементы конструкции здания, так и предметы интерьера, находящиеся в помещении.

В представлении большинства “заказчиков”, далёких от вопросов обеспечения безопасности и *просто плохо учивших физику в средней школе*, рентген является “универсальным средством” и с его помощью можно *“легко и просто”* проверить *(“просветить”)* “всё вокруг” – это **совсем не так**.

Портативные рентгенотелевизионные комплексы, используемые при проведении специальных проверок, имеют **ряд принципиальных особенностей**, связанных как с “технологией их функционирования”, так и с “медицинским аспектом” – поэтому они физически не могут быть задействованы для *“просвечивания всего вокруг”*.

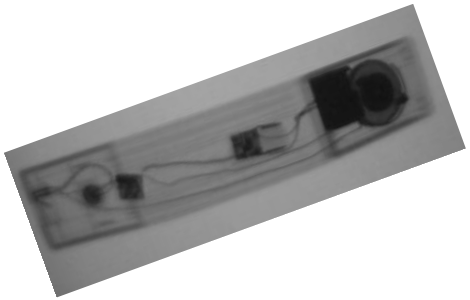
Что касается оценки результатов рентгеноскопии, то тут тоже много “нюансов” и всё зависит от подготовки оператора: одно дело, когда проверяется объект, в котором по определению ничего не должно быть – например, элемент мебели или мраморная статуя (*“целенькая, только без весла”* – как в песне у В. Высоцкого), и совсем другое дело – это проверка элементов, содержащих “штатную” электронику.

Немного о средствах рентгеноскопии.

Портативные рентгенотелевизионные установки построены по “модульному” принципу: блок-излучатель, “приёмный” блок, блок управления и обработки изображений.

www.teledyneicm.com

Пример использования портативной рентгенотелевизионной установки.



На сегодняшний день портативные рентгенотелевизионные установки практически отсутствуют в молдавском “коммерческо-частном поисковом секторе”.

Поэтому, уже сама фраза:
“мы используем для проверки вашего помещения рентген” –
звучит для молдавских “заказчиков” как чистый “развод”.

Как не попасть на “развод”: обязательный визуальный осмотр помещения.

Как было сказано ранее, у подавляющего большинства “заказчиков” представление о поиске устройств съёма информации связано только с использованием какого-либо специального оборудования – многие из них вообще убеждены в существовании *“чудо-приборов”*, которые *“всё найдут”*.

При этом “заказчики” даже не представляют *(или не хотят понимать)*, что **основная составляющая** поисковых работ – это тщательный **визуальный осмотр** проверяемого помещения.

Именно в ходе визуального осмотра можно обнаружить те средства съёма информации, на которые “не реагирует” поисковое оборудование: некоторые типы диктофонов и радиомикрофонов, некоторые проводные системы и т.п.

Естественно, что речь идёт о **настоящем визуальном осмотре** *(более подробно этот вопрос будет рассмотрен далее)*, а не об его “имитации”, когда *“специалист”* заглянул под стол и на шкаф – и всё.

Так что если “приглашённый специалист” в ходе поисковых работ не проводит тщательного визуального осмотра, а говорит, что он *“всё обнаружит с помощью своих приборов”* – то это “развод”.

Как не попасть на “развод”: комплексная специальная проверка помещения.

В то же время, одного “визуального осмотра” – *<u>даже “настоящего”</u>* – будет недостаточно для обнаружения некоторых угроз *(ниже приведены несколько примеров)*:

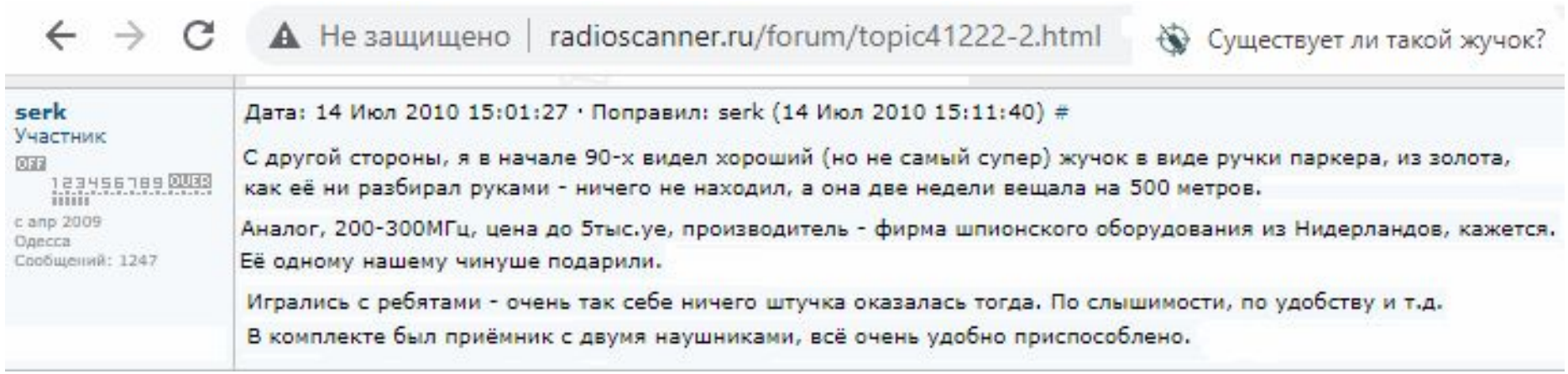
Форум на Analitika.info → Противодействие техническим средствам шпионажа. Поисковые мероприятия → О камуфляже

09.09.2010 14:26:52

Сообщение от **nemo**

О камуфляже

К вопросу о том - надо ли проверять нелинейником раскрытую вручную телефонную розетку?
Попалась разок в руки очень достойно сделаная (однозначно заводская) телефонная розетка советского стандарта с двойным дном. Причем ее основание было толще обычного на пару миллиметров и в глаза не бросалось. В пустоте - комбинированная закладка на 140 МГц. Антенна - само собой телефонная линия. Контакты к ней подпаяны с внутренней стороны и не видны абсолютно. Нашли нелинейником NR-900M



Как не попасть на “развод”: комплексная специальная проверка помещения.

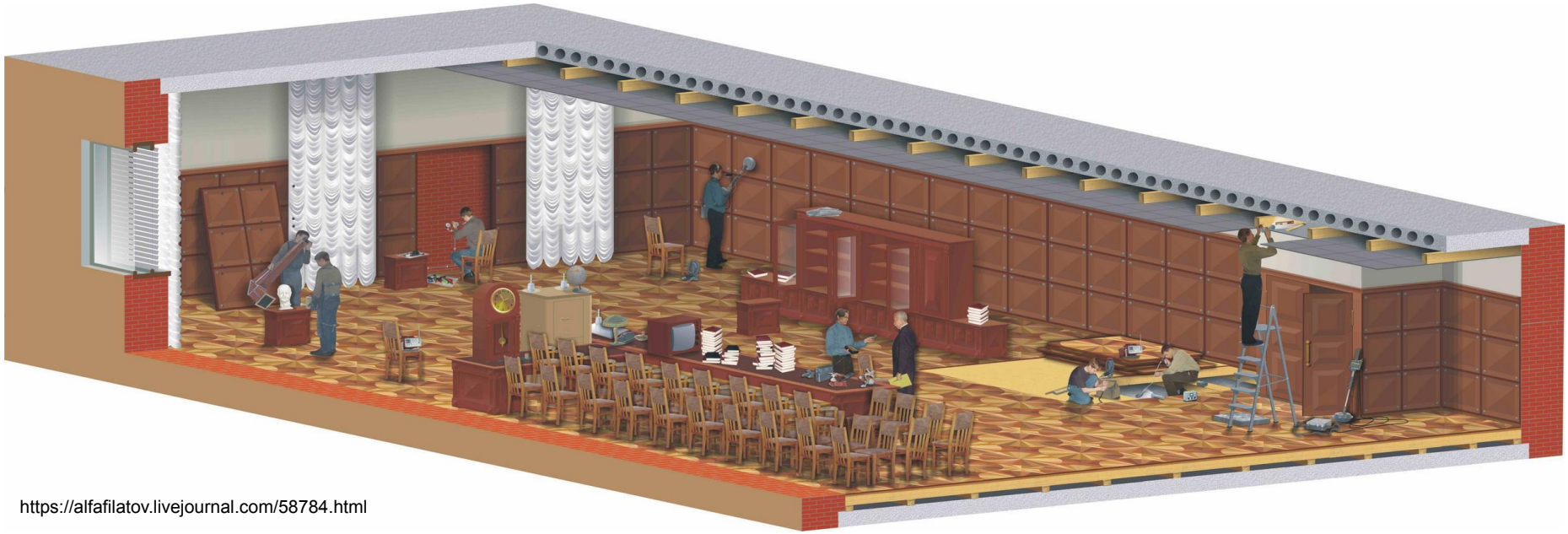
“Заказчик” должен чётко понимать, что для проведения **полноценной** специальной проверки **серьёзного** объекта необходимо выполнение целого **комплекса поисковых мероприятий**, при этом **обязательны**:

- тщательный визуальный осмотр помещения;
- проверка с помощью нелинейного локатора;
- проверка с помощью оптического обнаружителя видеокамер;
- проверка всех проводных линий с помощью специального анализатора;
- долговременный радиоконтроль *(минимум в течении нескольких дней)*;
- проверка отдельных элементов с помощью средств рентгеноскопии.

Кроме того, должны быть проведены работы по выявлению и оценке так называемых “естественных каналов утечки информации” различной физической природы, а также проверка средств вычислительной техники и телекоммуникационного оборудования на наличие “программных закладок” и “дополнительных функций”, которые могут стать причиной утечки информации.

*Пример проведения **настоящей** специальной проверки – см. далее.*

Пример проведения НАСТОЯЩЕЙ специальной проверки помещения.



https://alfafilatov.livejournal.com/58784.html

Специальная проверка, проводимая в помещении одной из дипломатических миссий СССР в середине 80-х годов.

Проверяется не только **каждый предмет мебели и интерьера**, но и **все ограждающие конструкции**:

полностью освобождается и сдвигается мебель, производится снятие паркета, демонтаж декоративных панелей со стен, вскрытие подвесного потолка и т.д. – “до бетона и кирпича” *(которые тоже проверяются)*.

Естественно, что <u>такая проверка длится не день и не два</u>.

Редкий случай – “приходящий специалист”, который задаёт вопросы.

В очень редких случаях может быть ситуация, когда “приходящий специалист” придёт вообще без каких-либо приборов и вместо того, чтобы рассказывать “какой он крутой поисковик” *(как делает большинство “специалистов”)*, он сам начнёт задавать множество вопросов и делать вещи, которые могут показаться “заказчику” странными и глупыми. Например, он попросит схему технических коммуникаций и электропитания здания; захочет поговорить с системным администратором (связистом) и электриком, которые обслуживают данный объект; попросит техническую документацию на офисную мини-АТС (причём *User Manual* его не устроит – ему будет нужен *Engineering Manual*); начнёт интересоваться, кто устанавливал и кто обслуживает систему ОПС и охранного видеонаблюдения. Но на этом он не остановится и захочет спуститься в подвал *(где находится электрощитовая)* и подняться на “технический этаж” *(куда приходят “вентиляционные короба”)*. В общем будет вести себя “крайне подозрительно” и “странно”.

В результате “заказчик” посмотрит на него и подумает: “Что это специалист по защите информации? Вместо того, чтобы *“колдовать”* с *“чудо-приборами”*, он по подвалам лазит и с электриком разговаривает…”. И, скорее всего, “пошлёт” этого специалиста. **А зря…**

Как не попасть на “развод”: обязательная “подготовительная работа”.

Именно так и должна начинаться настоящая проверка – вначале “поисковик” должен тщательно изучить объект проверки и уточнить все “нюансы”, на которые ему нужно будет обратить особое внимание в ходе работы.

Ну а к *“решительным специалистам”*, которые *“работают”* по принципу *“Пришёл. Увидел. Победил.”*, лучше отнестись осторожно – понятно, что каждый считает себя равным Юлию Цезарю или Александру Македонскому, но нужно смотреть на вещи реально…

Я уже не говорю про разработку “**модели нарушителя**” для проверяемого объекта или хотя бы составление “**плана проведения специальной проверки**”, который должен быть согласован с “заказчиком” –
об этих вещах *так называемые “специалисты”* вообще не имеют представления.

Так что “заказчик” должен понимать, что **для настоящей комплексной проверки объекта “приходящий специалист” должен провести серьёзную подготовительную работу**, которая на первый взгляд не видна.
В противном случае – очень велика вероятность, что вас “разводят”.

Примечание: естественно, что возможны разные ситуации – одно дело проверка вашей ванной комнаты и другое дело проверка крупного офисного здания – указанные выше замечания в первую очередь касаются проверки серьёзных объектов.

Требуйте от “приглашённого специалиста” документ по результатам проверки.

Очень важный и **принципиальный момент для “заказчика”**: после проведения специальной проверки **“приглашённый специалист” должен предоставить вам письменный отчёт** (*“акт”*, *“протокол”* – название документа может быть любое) **о результатах проделанной работы**.

В этом документе должны быть чётко указаны все виды работ, которые проводил “специалист” *(о минимальном перечне работ, которые должны быть выполнены при проведении полноценной проверки, говорилось ранее)*, используемое в ходе работ оборудование и результаты поиска.

Если со стороны “приглашённого специалиста” начнутся разные “отмазки” типа: *“Да это всё ерунда! Я специалист практической работы, а не бумажки пишу!”* – это типовой вариант “развода” и с очень высокой вероятностью *такой “специалист”* не только не умеет работать, но даже не понимает, что это такое.

Примечание: естественно, речь идёт о тех случаях, когда вы обращаетесь к “лицензированному специалисту”, от которого вы ожидаете качественное предоставление услуг.
Варианты, когда вы обратились к *“свободному художнику”* или к *“знакомому знакомого”*, который *“что-то умеет”* – даже не рассматриваются.

Помните о пословице: “Доверяй, но проверяй”.

Для того, чтобы проверить, на сколько добросовестно (качественно) работает “приглашённый специалист”, проводящий поисковые работы у вас на объекте, можно использовать различные “имитаторы устройств съёма информации”.

Причём для “имитации” закладного устройства можно использовать самые обычные бытовые предметы: кусок картона, маркер, батарейку, карточку СКУД, флэшку или карту памяти *(например, типа Microdrive)* и т.п., а так же камеры из старых *(не нужных)* мобильных телефонов.

Внешне такие изделия практически ничем не отличаются от реальных устройств съёма информации: например, картон или маркер – это типовые варианты камуфляжа “классических” радиомикрофонов, а флэшка, “пальчиковая” батарейка или карточка СКУД – это типовой вариант исполнения камуфлированного цифрового диктофона.

Примечание: *речь идёт об обычных бытовых предметах, которые только по внешнему виду похожи на некоторые устройства съёма информации и могут использоваться в качестве их “визуальных имитаторов” – не путать с многофункциональными имитаторами сигналов типа “Аврора”, “Импульс”, “Шиповник” и т.п.*

Далее приведены фотографии некоторых бытовых предметов, которые могут быть использованы в качестве “проверочных имитаторов”.

Примеры “имитаторов” устройств съёма информации.

Использование “имитаторов” устройств съёма информации.

Установить “имитаторы” нужно с “умом и фантазией” – т.е. так, чтобы с одной стороны они находились в местах возможной установки реальных устройств съёма информации, а с другой стороны – если “приглашённый специалист” их обнаружит, то у него не должно возникнуть подозрения, что его “проверяют”.

Например, если спрятать флэшку или карточку СКУД за подвесным потолком, то это будет не совсем “реалистично” *(если их там найдут)*, а вот кусок картона, который лежит за подвесным потолком (как “строительный мусор”) – это вполне реальная картина.

Другой пример: если спрятать флэшку или маркер внутри пластикового кабель-канала, то это будет явный “перебор” – *если только вы не собираетесь в открытую сказать “приглашённому специалисту”, что вы его проверяете*.

В то же время: флэшка в “кармане” мягкой игрушке *(ребёнок игрался)*, карточка СКУД между страницами книги *(читал и оставил её там как закладку для книг)* или маркер, “упавший” в щель между подушками кресла или дивана – всё это вполне реальные жизненные ситуации.

Далее приведены несколько примеров возможного размещения “проверочных имитаторов”.

Примеры “имитаторов” устройств съёма информации.

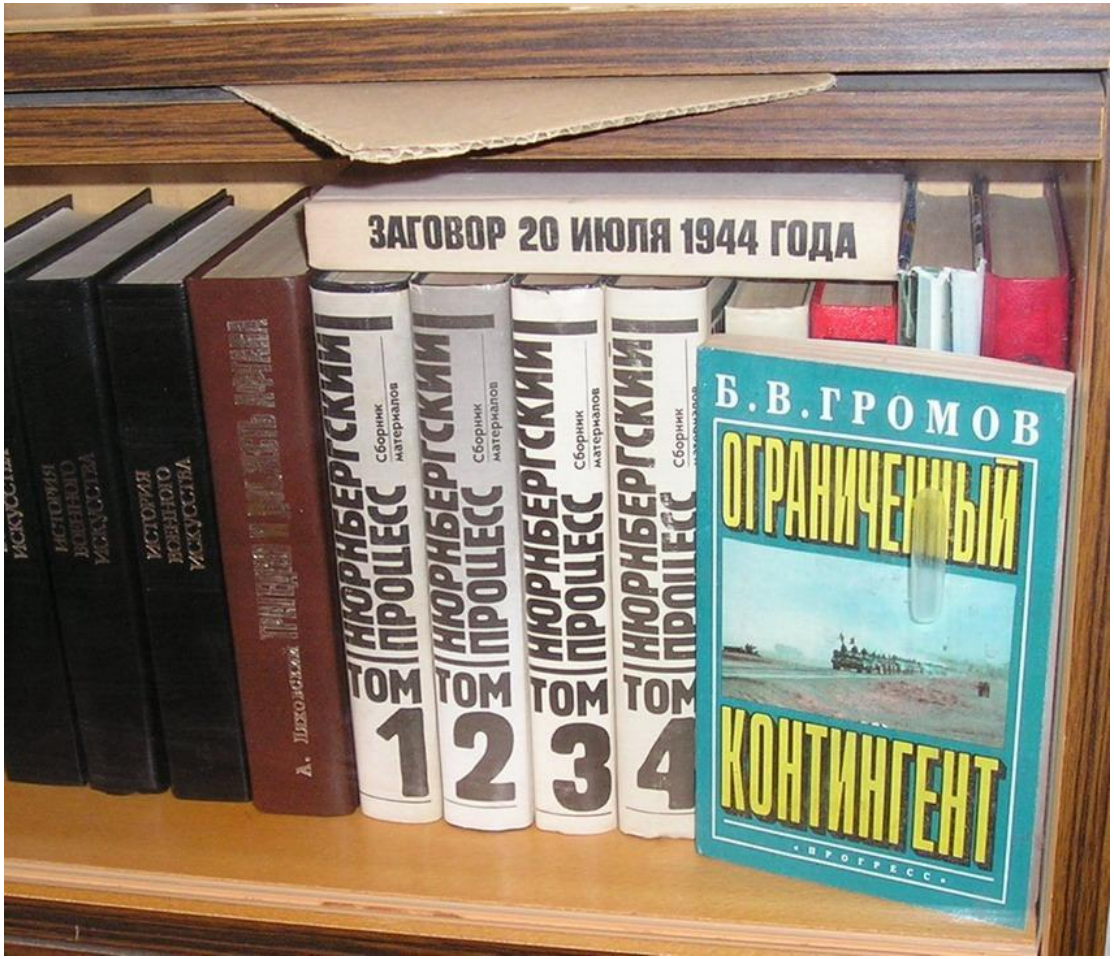
Камера от мобильного телефона, установленная на сувенире.

Ваша реакция, если её найдут: “А-а-а! Это ребёнок поставил, когда играл, – будто бы это туристка с фотоаппаратом”.

Примеры “имитаторов” устройств съёма информации.

Картонка, “валяющаяся” где-то под диваном.
Ваша реакция, если её найдут: “Вот бардак! Совсем не убирают помещение!”.

Примеры “имитаторов” устройств съёма информации.



Картонка между книжными полками (должна быть задвинута в самую глубину).
Ваша реакция, если её найдут: “А-а-а! Она там лежит как прокладка”.
Для реалистичности можно поставить по куску картона между всеми полками.

Примеры “имитаторов” устройств съёма информации.

Картонка
между “стыками” мебели
(должна быть задвинута).
Ваша реакция, если её найдут:
“Она там лежит как прокладка”.

Примеры “имитаторов” устройств съёма информации.

Картонка под днищем раздвижного стола (должна быть задвинута).

Примеры “имитаторов” устройств съёма информации.

Карта памяти, “сдвинутая” под телевизор или другой предмет интерьера. Ваша реакция, если её найдут: “Вот она где была! Спасибо! Я её ищу три дня!”.

Примеры “имитаторов” устройств съёма информации.

Маркер, “упавший” в диван, и флэшка в “кармане” мягкой игрушки.
Ваша реакция, если их найдут: “А-а-а! Вот куда он (она) затерялись!”.

Примеры “имитаторов” устройств съёма информации.

Батарейка, “упавшая” в кресло – должна быть закрыта “подушками”, чтобы её не было видно.
Ваша реакция, если её найдут: “Видно провалилась случайно”.

Примеры “имитаторов” устройств съёма информации.

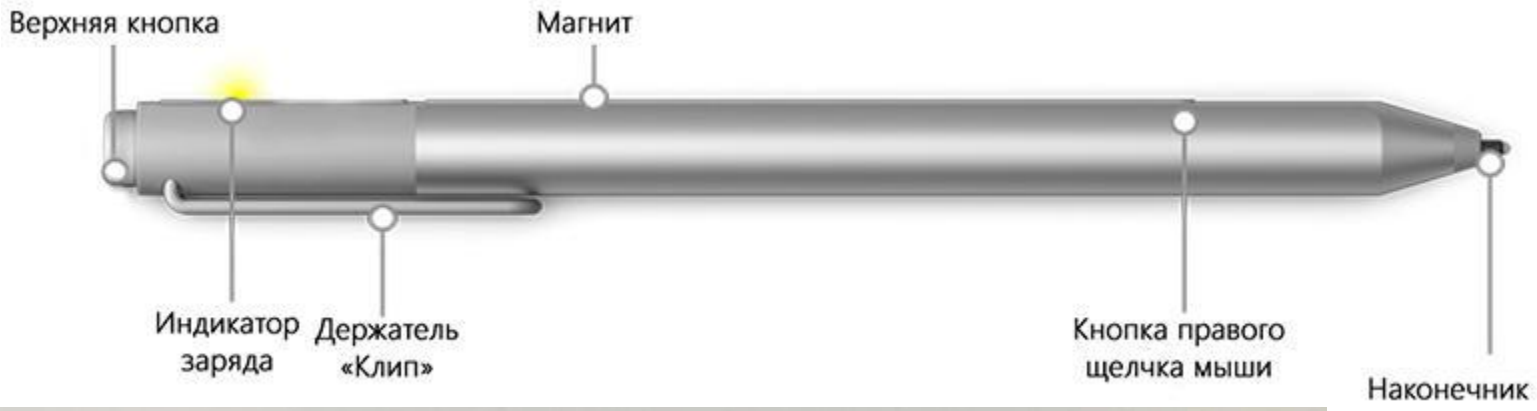
Карточка СКУД, лежащая между страницами книги – на фотографии “условное” положение – карточка должна находиться внутри книги между страниц.

Ваша реакция, если её найдут: “А-а-а! Это не рабочая карточка, я её использовал как закладку для страниц, когда читал книгу”.

Примеры “имитаторов” устройств съёма информации.

Карточка СКУД под днищем стола (должна быть задвинута).
Если её найдут, то придумайте сами, что сказать.

Стилус для планшета – идеальный “имитатор” устройств съёма информации.



Идеальным “имитатором” устройств съёма информации является стилус для планшета. Данное изделие должно просто лежать среди ручек и карандашей – например, в ящике рабочего стола или в “стакане”.

“Приглашённый специалист” **обязан обнаружить его** – *т.е. идентифицировать, что это не “авторучка”, а изделие, содержащие в себе электронные компоненты* – с помощью нелинейного локатора или в ходе визуального осмотра предметов интерьера.

Небольшой “итог” по поводу “приглашённого специалиста”.

Если “приглашённый специалист” в ходе проведения поисковых работ найдёт ваши *“контрольки”*, то это уже хорошо и с ним можно о чём-то говорить. Если же он их не найдёт, то это была не “проверка помещения”, а самая обыкновенная “шара” – причём с большой буквы “Ш”: “Шара!” – даже не “с большой буквы”, а всё слово “большими буквами”: “**ШАРА!**”.

Нужно чётко понимать, что при проведении **настоящей** специальной проверки “приглашённый специалист” должен осмотреть и исследовать не только **каждый** предмет интерьера, находящийся в проверяемом помещении, но и **каждый** элемент конструкции данного помещения.

В итоге хочется дать простой, но очень полезный совет “заказчикам”, которые решили обратиться к “специалистам по поиску устройств съёма информации”: чтобы вас не “развели” и не “кинули”, нужно прежде всего ДУМАТЬ, а не “вестись” на рассказы про *“чудо-аппараты”* и *“секретные технологии”* – даже если их вам рассказывают с *“умным видом”*.

И всегда помните фразу из фильма “**Тот самый Мюнхгаузен**”:
“Умное лицо – это ещё не признак ума, господа.
Все глупости на земле делаются именно с этим выражением лица!”.

Некоторые размышления о “перспективах поискового бизнеса”.

Кратер
Участник
с апр 2007
Харьков

А вообще каковы перспективы развития поискового бизнеса в РФ и Украине? Стоит ли этим заниматься на коммерческой основе, разумеется официально?

Fath
Участник
с мая 2007
Ярославль
Сообщений: 1760

Дата: 19 Дек 2010 20:23:55 · Поправил: Fath (19 Дек 2010 20:25:30) #

Кратер
Как Вам сказать - если брать по регионам и брать чисто коммерческую составляющую, то не думаю, что доходность данного бизнеса будет высокой. В это дело только на стадии открытия нужно вложить порядка 3 млн. руб., да и то уже на некоторой готовой базе. С мероприятия Вы будете получать ну пусть тысяч 100, а если учесть, что абсолютное большинство желающих провести такое действо, узнав ценники моментально пересматривают свои взгляды на обеспечение информационной безопасности, то даже чисто окупить затраты будет не совсем просто.

Тут два выхода:
1. Вы начиаете работать в каком ни будь перспективном регионе, который достаточно удалён от Москвы, где рынок данных услуг ещё не представлен, а потребности есть, там Вы начинаете дело, отбиваете затраты, завоёвываете себе репутацию и место на рынке.

2. Вы сильно дружите с определёнными структурами, предприятиями и т.п., которые заинтересованы в получении такого рода услуг, и открываете свой бизнес чисто под них, хотя бы для начала. Ну про всякие там крыши и связи я не говорю.

Есть так же вероятность того, что когда ни будь выйдет некое постановление, которое обяжет все учреждения, занимающиеся определённым родом деятельности, проводить на своих объектах поисковые мероприятия (ну вот наподобие того, что сейчас с персональными данными). Ну тут уж главное вовремя подсуетиться (ну и опять таки - крыши, связи...).

Ну и можно ещё заниматься откровенным кидаловом или около того, проводя какие-то мутные манипуляции и выдавая какие-то мутные рекомендации. Так народ тоже работает.

(Замечу, что это сугубо мои личные соображения).

Zet
Участник
с июл 2006
Петропавловск-Камчатский
Сообщений: 557

Дата: 20 Дек 2010 11:53:14 #

Fath

каком ни будь перспективном регионе, который достаточно удалён от Москвы, где рынок данных услуг ещё не представлен, а потребности есть,

Эх где ныне можно найти такой перспективный регион. Где действует успешные коммерческие предприятия (не гос. организации, корпорации), которые готовы эти услуги потреблять и оплачивать.

Кратер

А вообще каковы перспективы развития поискового бизнеса в РФ и Украине?

Лучше Вы нам расскажите какие перспективы у этого бизнеса в Украине.

Кратер
Участник
с апр 2007
Харьков

Дата: 20 Дек 2010 11:58:35 #

После принятия нового налогового кодекса уже никакая, хотя и раньше была не радужная. Раньше гос объекты могли себе иногда позволить атестоваться, а сейчас у гос нет денег, а комерсы и банки действуют по своему усмотрению, одним словом не до информационной безопасности им сейчас, все сворачивается и сокращается.

Кратер
Участник

Дата: 20 Дек 2010 16:52:33 #

Такие мысли были по организации, но пока будущего не вижу у нее, одни убытки

Реальное положение дел на сегодняшний день в Молдове *(моё личное мнение)* – выделено чёрным.

Небольшой “итог” по поводу ситуации, связанной с предоставлением “поисковых услуг” в Молдове – *моё личное мнение*.

На сегодняшний день в Молдове ситуация, связанная с предоставлением услуг по поиску устройств съёма информации в частности и по технической защите информации в целом, находится где-то на начальном этапе развития – *речь идёт о “коммерческо-частном секторе”*.

Например, в Республике практически нет компаний, которые могут предоставить и качественно выполнить **весь** перечень мероприятий, необходимых для проведения **полноценной** специальной проверки.

Это понятно – в Молдове никто не будет вкладывать порядка **100 000 USD** на приобретение настоящего поискового оборудования и подготовку настоящих специалистов, так как эти затраты никогда не окупятся на местном рынке.

Я уже не говорю о “методологической” составляющей: утверждённый перечень необходимого оборудования, наличие *(вернее отсутствие)* в Республике утверждённых методик поиска (многие *т.н. “специалисты”* путают их с “Инструкцией по эксплуатации” на имеющиеся у них приборы) и т.д.

Примечание: как было сказано ранее, речь идёт о “лицензированных специалистах”, от которых вы ожидаете качественное предоставление услуг и гарантию качества выполненных работ. Варианты, когда вы обратились к *“свободному художнику”* или к *“знакомому знакомого”*, который *“что-то умеет”* – даже не рассматриваются.

Небольшой “итог” по поводу ситуации, связанной с предоставлением “поисковых услуг” в Молдове – *моё личное мнение*.

Так что на сегодняшний день в молдавском “коммерческо-частном секторе” практически никто не может решить “**комплексную задачу**” по поиску возможно внедрённых устройств съёма информации.

В то же время, с большей или меньшей вероятностью могут быть решены некоторые “**частные задачи**”: например, связанные с обнаружением скрытых видеокамер и некоторых типов радиомикрофонов, работающих “на передачу” в момент проведения проверки, а также ряда других “заносных” средств съёма информации. Эффективность решения этих “частных задач” зависит от профессионализма и технического оснащения соответствующих “поисковиков”.

Всё это необходимо чётко понимать потенциальным “заказчикам” данного вида услуг при обращении в соответствующую компанию. Естественно, что **различного рода *“частные детективы”*** или ***“радиолюбители-самоучки”*** *с “чудо-приборами”, сделанными по книге “Шпионские штучки”,* – **это просто клоунада**.

При обращении **“заказчик” должен получить чёткий ответ** о том, **что реально могут сделать данные “поисковики”**: что они могут сделать “точно”, что они могут сделать “с определённой вероятностью” и чего они не могут сделать в принципе.

Как было отмечено ранее, если “заказчику” скажут, что-то типа: *“мы самые лучшие”* и *“мы можем обнаружить любые устройства съёма информации”*, то ему нужно сразу очень хорошо задуматься – ***так ли это на самом деле****?*

Что в итоге?

В итоге у многих может возникнуть логичный вопрос: если всё действительно так плохо, как было изложено выше, то что тогда делать – получается, что обращаться к “поисковикам” вообще нет смысла?

Не совсем так. Да, явных “шаровиков” нужно отбросить сразу. Причём многие из них сами не захотят с вами связываться, если увидят, что вы задаёте им конкретные “наводящие вопросы” по поводу предстоящей проверки и реально пытаетесь проверить их компетентность.

С теми же “поисковиками”, которые честно скажут о своих **реальных** возможностях, можно попробовать работать – не забывая про правило: *“Доверяй, но проверяй”*.

При этом нужно чётко понимать, что в каждом конкретном случае исходя из **реально возможных** угроз, очень важно правильно выбрать соответствующую *“глубину проверки”*, которая реально необходима именно для данного объекта – как говорится: *“Кесарю – кесарево, а слесарю – слесарево”*.

Конечно же можно считать себя *“особо важной персоной”* – *именно так думает о себе подавляющее большинство “заказчиков”* – и при обращении к “поисковикам” поставить им задачу *“найти всё, что только может быть”*.

Но, как было уже сказано *(моё личное мнение)*, на сегодняшний день в молдавском “коммерческо-частном секторе” не существует “поисковиков”, которые **реально** способны выполнить такую задачу.

Что в итоге?

При этом нужно помнить, что защита информации – это целый комплекс мер, в котором "поисковые вопросы" не самые главные *(моё личное мнение)*.
Если говорить о защите акустической *(речевой)* и видовой информации от утечки по техническим каналам, то основную роль в их защите играют **организационно-режимные меры** – около **50%**, далее идут защитные мероприятия с использованием **технических средств защиты информации** – около **30%** и только потом идут непосредственно **"поисковые" мероприятия** – около **20%** *(это моё личное мнение, причём достаточно спорное – имейте это в виду)*.

Если вам повезло *(что бывает очень редко)* и вы пригласили действительно более-менее грамотного специалиста, то он после проведения проверки, исходя из конкретной **реальной** ситуации, должен чётко сказать о тех угрозах, которые он не может обнаружить или которые существуют *"по определению"*, и должен дать определённые рекомендации, направленные на их устранение или максимальное уменьшение.
Другое дело, что эти рекомендации должны быть действительно грамотными и реальными, а не рассказами о *"чудо-коробочке, которая защитит от всего"* (немного подробнее об этом будет сказано в конце презентации).

Так что, как было сказано ранее: *"Чудес в защите информации не существует"* – **защита информации это ежедневная многоплановая работа**.

Некоторые вопросы, связанные с ситуацией, когда проведением специальных проверок занимается не “человек со стороны”, а “свой” сотрудник.

– На кого?!

*– Да, да, на Штирлица. Единственный человек в разведке Шелленберга, к которому я относился с симпатией. **Не лизоблюд**, спокойный мужик, без истерик и **без показного рвения**.*
*Не очень-то я верю тем, кто вертится вокруг начальства и выступает без нужды на наших митингах – **бездари, болтуны, бездельники**…*
А он молчун. Я люблю молчунов… Если друг молчун – это друг.
Ну а уж если враг – так это враг. Я таких врагов уважаю.
У них есть чему поучиться…

Юлиан Семёнов, “Семнадцать мгновений весны”.

Вариант, когда вопросами защиты информации будет заниматься не “приглашённый специалист”, а ваш сотрудник.

Ранее был рассмотрен вариант, когда для проведения работ по защите информации *(в частности, для поиска устройств съёма информации)* приглашался “специалист со стороны”, и были даны некоторые рекомендации относительно предотвращения возможного “развода”.

В то же время, возможен и другой вариант – *как было сказано, для Молдовы достаточно редкий* – когда вопросами защиты информации поручено заниматься непосредственно сотрудникам компании:
или “штатно”, или “в нагрузку” к их основным обязанностям.
Кроме того, этот вариант касается отдельно взятых граждан, которые самостоятельно занимаются защитой своих “личных секретов”.

Здесь тоже есть определённые “нюансы”, связанные с тем,
чтобы эта **работа выполнялась реально и эффективно, а не была просто “имитацией бурной деятельности”** – не важно по какой причине:
из-за некомпетентности *(бестолковости)* сотрудника или из-за того,
что он просто “забил” на работу.

Некомпетентный сотрудник *(работник-дурак)* – хуже любого “внешнего” врага.

Проблема некомпетентности *(бестолковости)* сотрудников была, есть и будет всегда – *речь идёт именно о “своих” сотрудниках, работающих в компании*.

Очень хорошо о такой ситуация сказано в повести “**В полосе отчуждения**”, (авторы – А.Безуглов и Ю.Кларов):

Нет, не жулик, хуже – просто дурак.
Убытков на десятки тысяч рублей золотом, а виновных нет:
недоучли, недоглядели, недосмотрели, недодумали.
А какой с дурака спрос? Знают, что дурака не наказывают.
Дураку сочувствуют – свой дурак, привычный.
Быть дураком – почти что капитал иметь: пустил в оборот и
жди себе процентов. С обычной дурости – пять годовых.
С дремучей, глядишь, и все десять накапает…
А от него – от дурака, если хочешь знать, вреда побольше,
чем от всех других врагов вместе взятых. А цацкаемся.
И что обидно – кормят-то нашего дурака не из-за кордона, а мы сами.
И кормим, и одеваем, и обуваем, и должности даём, а придётся –
то и награды. Живи, дурак, плодись, веселись! Почёт тебе и уважение!

Вот такие дела… Думаю, что многие с этим сталкиваются постоянно.

Две типовые проблемы: некомпетентный сотрудник *(работник-дурак)* и сотрудник, который “забил” на работу.

Поэтому вопрос профессионализма “своих” сотрудников, отвечающих за защиту информации *(в частности, за поиск устройств съёма информации)*, является очень актуальным и требует от работодателя серьёзного и грамотного подхода как к подбору сотрудников, так и к обеспечению их первичной подготовки и последующей периодической переподготовки – *при этом нужно помнить очень хорошую фразу: “Учиться никогда не поздно, но иногда – бесполезно”*.

Другая проблема связана с ситуацией, когда даже более-менее грамотный специалист начинает “расслабляться” и относиться к своим обязанностям не как к выполнению “боевой задачи” *(образно говоря)*, а как к формальной и “показушной” деятельности – типа: *“Да что тут может быть? В Багдаде всё спокойно!”*.

В результате в обоих случаях получается, что реальная работа превращается просто в *“имитацию бурной деятельности”*.

Далее рассмотрим некоторые “типовые” проблемы, которые возникают при создании “своего” подразделения по технической защите информации. Этот вопрос достаточно подробно обсуждался на форуме сайта www.analitika.info – так что *“цитирую первоисточник”*, добавляя свои *“комментарии” (см. далее)*.

Типовые вопросы, возникающие при создании “своего” подразделения ТЗИ.

Не защищено | forum.analitika.info/viewtopic.php?id=46

Сообщение от **nemo** 21, December, 2006 23:23
Оснащение поисковой бригады

В данной теме предлагаю затронуть такой вопрос - поставленна задача на предприятии создать подразделение ПДТСР (противодействия техническим средствам разведки). Одна из основных задач подразделения - периодические проверки по выявлению закладных устройств. **Чем бы Вы укомплектовали такое подразделение и почему?**

Дабы все не свести к разговору "нет денег" рассмотрим три случая

1. Небольшая фирма - десяток кабинетов, и одному сотруднику поставили задачу - ищи. Что искать - сами пока не знают
2. Подразделение на предприятии. Деньги дают, но без фанатизма. Проверки раз-два в месяц
3. Крупная компания с филиалами и все по взрослому. Надо - делайте все, что положено. Проверки каждую неделю, перед ответственными мероприятиями, выезды в филиалы

Сообщение от **serge331** 24, December, 2006 23:40
Re: Оснащение поисковой бригады

Ну вы, блин даете! См. предыдущий форум!
Анекдот такой есть. Сняли в советской время одного директора, а на его место назначили нового. Идет передача дел. И под конец сели они, выпили и старый дает молодому три заклееных конверта. "Открывай,-говорит, - их по очереди, когда будет совсем хреново..."
Прошло полгода. План завален. Молодой открывает первый конверт. Там написано:"Вали все на меня".
Прошло 2 года. Все равно ситуация не выправляется, завод лихорадит. Окрывает второй. Там:"Проводи реорганизацию".
Бьется молодой третий год, а результата так и нет. Открывает он последний конверт. А там:"Пиши три конверта".
В отношении темы в Вашей редакции это, по моему так:
1. Можно прочитать книги Хорева и Маркыча и ни хрена не делать.
2. Обратиться к друзьям-специалистам.
3. Валить из этой компании под благовидным предлогом, не забывая упоминать ее в резюме при поиске работы.
Повеселили, спасибо.
С пожеланием успехов.

Сообщение от **nemo** 25, December, 2006 00:06
вот что получается

Ну вот и без всяких подводов сразу попали в точку.Прям что хотел, то и получил.
Итак действительно мое мнение почти такое же, но только с меньшим цинизмом
1. Не нужно им никакое оборудование для поисковой бригады. Провести комплекс орг мероприятий, Закрыть имеющиеся каналы утечки и как и во втором случае - вызывать планово и вне планово бригады со стороны.
2. Тут уже не факт что друзья спецы подойдут. Если деньги есть и не считаются - да. А если действительно пара проверок в месяц. Пусть каждый раз проверяется помещение 20 квадратов х20(30)$ = 400(600)у.е. в месяц до 1000 у.е. Хм - за год уже сумма набегает. Одним словом если есть кого обучать и кому отверткой крутить - может и нужны свои поисковики. Считать надо
3. Почему валить? Напряженная работа? Некоторым нравится. Вопрос медицины при работе с НЛ сугубо индивидуальный

На мой взгляд, типичная ситуация для большинства компаний (в том числе достаточно крупных): “**… одному сотруднику поставили задачу – ищи. Что искать – сами пока не знают**” – уверен, что многие сталкивались именно с такой “постановкой задачи”.

Типовые вопросы, возникающие при создании “своего” подразделения ТЗИ.

Не защищено | forum.analitika.info/viewtopic.php?id=46

Сообщение от **serge331** 20, January, 2007 23:29
Re: Оснащение поисковой бригады

Вечер добрый!
Все еще более цинично:
1. Можно ни хрена не делать вообще, а только дуть щеки. Ну на худой конец купит это, как его.... А! Интерсептор! Кстати автоматический перепер английского не всегда грамотно переводит суть. Помните фильм "Perfect Storm", который в нашем прокате шел под именем "Идеальный шторм"? Перевод не напрягает? Праальна!
Ну прям мастурбатор с педальным приводом. Ну так вот. Со вторым словом вроде склалось, а вот с первым - беда! Есть еще значение. Можно матерное:о...й.
Если напрячься, то можно перевести как "Шторм века". Отвлекся, мля! Так вот!
Интерсептор- значить частотомер с расширенными возможностями. Лучше всего, не сочтите за рекламу "РИЧ-3". Если совсем худо с баблом, то подержанный "второй".
Это самая грамотная машина на рынке. Чувствуется, что задумана еще в советские времена. И реализация, как часто бывает, не испохабила идею.
Далее следует внимательно прочитать инструкцию и поочередно ставить в кабинеты. Если что-то есть, то непременно зацепите.
Да! Забыл, что в любом случае подразумевается хотя бы среднее радиотехническое образование.

2.Если для конторы 12 штук зелени в год- проблема, то у нее нечего тырить. Особенно с использованием техсредств. А друзьям- спецам следует позвонить и посоветоваться как грамотно организовать "технический режим". И не более того. Кстати, сколько же Вы намерены платить штатному спецу в этом случае?! Грамотный практик не одну штуку стоит! Режим дополните простеньким автоматизированным радиоконтролем, но пригласите спеца разгребать результаты. Повторюсь, но в умелых руках и х... - балалайка!

3. Если контора серьезная, а у Вас есть вопросы типа "как", "что" и "почему", валить надо как можно быстрее. Потому как всерьез можно схлопотать от своих же по репе за некомпетентность, т.е. за утечку информации. Или искать пенсов, у которых, как тут хорошо сказано, "25 лет в КГБ на лбу написано".
По крайней мере они подскажут как грамотно потратить деньги, организовать работу, прикрыть явные дыры и свою жопу (что самое важное).

Кстати думаю, что скоро вернутся в плане использования техники для получения информации восьмидесятые годы. Уж больно все стало доступно. И умников (в хорошем смысле) много стало. А умники-то они жадные по первости и одновременно глупые... Но кто выживает и попадает в хорошие руки, тот очень скоро становится настоящим волком.

С пожеланием успехов!

Сообщение от **serge331** 22, January, 2007 18:13
Re: Оснащение поисковой бригады

Вечер добрый!
Грамотный оператор комплекса радиоконтроля птица еще более редкая, чем грамотный поисковик. Насколько я знаю, в начале прошлого года искала одна солидная контора такого собственного спеца. Клали ему от 35 тыс. руб. в мес. Но за полгода так и не нашли. И пришлось им заключать договор с фирмой - производителем.
Ну а сколько стоит "технический специалист по безопасности" с "25 годами на лице"... Все зависит от круга обязанностей.
Некоторые "хозяева" начитаются книжек и насмотрются фильмов - и ну фантазировать! Но лично я придерживаюсь политики "за Ваши деньги- любой каприз!". Ну.. почти любой.
С пожеланием успехов.

Каждую фразу можно практически “разобрать на цитаты” – всё один в один, как есть на самом деле в реальной жизни – *некоторые мои “комментарии” см. далее*.

Примечание: цитируемые сообщения были в 2007 году *(см. даты)* – поэтому указанные в них образцы техники (“РИЧ-3” и “РИЧ-2”, да и вообще “интерсептор” как таковой) актуальны на тот период – сейчас ситуация в области радиоконтроля принципиально изменилась.

Принципиальный “комментарий”.

“Если для конторы 12 штук зелени в год – проблема, то у неё нечего тырить. Особенно с использованием технических средств.” – абсолютно согласен.

Но хочу сделать небольшое, но принципиальное замечание: это верно, если речь идёт именно о “вопросах бизнеса” – т.е. в случае “классического” промышленного шпионажа.

В то же время, возможны различные другие ситуации, когда “объектом разведки” может быть не только “юридическое лицо” (причём от крупной компании до “индивидуального предприятия”), но и любое “физическое лицо” – при этом мотивы “злоумышленника” могут быть самые разные: криминальные элементы *(в процессе подготовки преступления)*, сбор компромата, “папарацци”, личная вражда или месть, варианты “муж - жена” или “любовник - любовница”, вариант “просто поприкалываться” *(“набрать лайков”) – очень актуально сейчас* и т.д.

Кроме того нужно помнить, что сейчас появилось большое количество “бытовых устройств” *(смартфоны, “планшеты”, миниатюрные цифровые диктофоны, видеорегистраторы и т.д.)*, которые доступны всем, но вполне могут быть использованы для аудио- и видеозаписи.

Так что не стоит забывать хорошую фразу из *“**Семнадцати мгновений весны**”*:
“*Я не хочу будить в вас злобную химеру подозрительности по отношению к товарищам по партии и по совместной борьбе, но факты говорят о следующем*…”.

Поэтому впадать в “шпиономанию” конечно же не стоит, но нужно реально оценить “факты” и действовать исходя из конкретной ситуации – во многих случаях проведение каких-либо “специальных проверок” вообще не понадобится и все “проблемы” можно будет решить с помощью организационно-режимных мер *(в основном “правильным поведением”)*, а в ряде случаев может понадобиться реальная работа именно по технической защите информации.

Некоторые “комментарии”.

“Можно … только дуть щёки.” – многие *так называемые “специалисты”* именно так и “*работают*”.

“Грамотный практик не одну штуку стоит!” – это верно, но вопрос в том, чтобы это был действительно “грамотный практик” в области ТЗИ – а таких в Молдове…
(да и не только в Молдове).

“Грамотный оператор комплекса радиоконтроля – птица ещё более редкая, чем грамотный поисковик.” – *см. предыдущий “комментарий”*.

Что касается **“пенсионеров, у которых 25 лет в КГБ на лбу написано”** – тут не всё так просто.
Есть очень хорошая поговорка: *“Не нужно путать опыт работы со стажем”*.
Так что если “25 лет реального опыта работы” – это да! А если “25 лет стажа” – это совсем не то.

“Некоторые “хозяева” начитаются книжек и насмотрются фильмов – и ну фантазировать!” – тут невольно вспоминается аналогичная фраза Мюллера из “***Семнадцати мгновений весны***”:

“Меня сегодня вызвал шеф. Они все фантазёры, наши шефы…
Им можно фантазировать – у них нет конкретной работы, а давать руководящие указания умеет даже шимпанзе в цирке…”.

Конечно, не ко всем “шефам” это относится, но…

Вообще адекватный и думающий “шеф”, которому можно спокойно объяснить суть проблемы и предложить грамотное решение, которое в дальнейшем будет реально реализовано и будет реально выполняться *(в первую очередь будет выполняться самим “шефом”)*, – это большая удача для сотрудника, отвечающего за защиту информации.

Типовые вопросы, возникающие при создании “своего” подразделения ТЗИ.

Не защищено | forum.analitika.info/viewtopic.php?id=46

Сообщение от **egor** 23, January, 2007 05:39
Re: Оснащение поисковой бригады

Нагло встряну в беседу профессионалов.

"Если для конторы 12 штук зелени в год - проблема, то у нее нечего тырить". В общем-то верно, ну а как быть с госструктурами? Скажем финансовыми. Информация о траншах, кредитах, крупных госзакупках есть серьезная информация. С одной стороны вваливаются неправдоподобные баблы на аттестации, защиту сетей и пр. С другой - совершенно формальный подход к внутреннему нарушителю, модель которго, кстати, заставляют рисовать. На поисковое оборудование деньги можно выцыганить только при условии, что сильно напугаешь начальство. Что бывает редко, т.к. крупное начальство свято верит в свою непокобелимость. Пока коллегу не посадят.

С другой стороны - некая структура негосударственная. В некотором царстве. Не буду называть, но, скажем, сильно богатая. Ну очень сильно, не Лукойл какой-нить. Денег на безопасность не жалеют. Читают рекламу, забивают в план годовой все, что видят - и попробуй не освой денюжку. При этом безопасники сидят на другом конце города от основной конторы и бомбят ея оттелева всевозможными директивами. Однажды вскрывается, что кто-то на их инет-трафике пасется, качает че-то на халяву. Задергались, вычислили - из информотдела парнишка под их IP-шником лазил. Долго бычились, парень в отказ ушел, уволили приказом, он в суд подал. Доказать не удалось, пришлось компенсировать и брать назад, а поскольку должность прежняя его уже занята была взяли куда? Правильно, к безопасникам. Типа пусть в отстойнике сем посидит, пока нормальная вакансия будет. Короче, в неумелых руках и балалайка - ...й.

Тут уважаемый 331 намекал, что имеет отношение к принятию решений по техническим параметрам замеров по аттестации. Долго ругались про необходимость этой самой аттестации и т.д. А вот интересует мнение человека, каким-то боком относящегося к технической политике - чё-нить изменится насчет поисковых мероприятий, оснащения техникой, нормального обучения для казенных контор, может быть расширения прав служб безопасности и т.д? Хотя конечно последнее весьма спорно, скажут - в органы обращайтесь, да и все.

Или так по гроб жизни на ...ю бренчать, а балалайкой тыкать?

Не, мужики, честное пионерское, без подкалывания. Интересно просто.

Сообщение от **serge331** 23, January, 2007 20:50
Re: Оснащение поисковой бригады

Вечер добрый!

Это недостатки существующего законодательства. Если одни нормы носят характер постановления правительства, т.е. предписывающий характер, определены критерии информации и предусмотрена как административная , так и уголовная ответственность за нарушения, то другие,СТР-К например, носят рекомендательный характер.

А в части защиты утечки конфиденциальной информации по техническим каналам требования вообще не определены.Так что коллегу протите сажать не за что. Оштрафовать или посадить его могут только за злоупотребления служебным положением и т.д. по постановлению суда в соответствии с действующим административным или уголовным кодексом.

Причем в нормах написано, что меры по защите конфиденциальной информации определяются организацией, которая является владельцем информационного ресурса.

Выдает директор приказ - так достаточно, и усе. Норм-то нету. Он и деньги-то законно потратить на это не может. Ведь не гостайна.

Теперь Ваш пример о частниках. Знакомая ситуация. СБ возглавляют бывшие менты или прокурорские. Там методы работы чисто оперативно-административные с использованием наработаннных годами связей и круговой поруки. Ну вообщем все ясно. О технике там имеют чисто умозрительные заключения. НУ и т.д.

Так что, грубо говоря, это все зависит от того, кто крышует. Грамотные и сбалансированные СБ есть очень не многих даже богатых контор. Все, по-моему, определяется их происхождением.

Теперь о единых требованиях....На просторах нашей страны они не будут соблюдаться в ближайшем обозримом будущем по причине невозможности их выполнения в нашем государстве на настоящем этапе его развития.Бедные мы.Причем не материально. Средства у нас есть, а вот ума... Сложно? Да нет, все просто. Как и во всем. Как исполнение ПДД.

Так что обращайтесь в органы, которые являются суть плотью от плоти нашей.

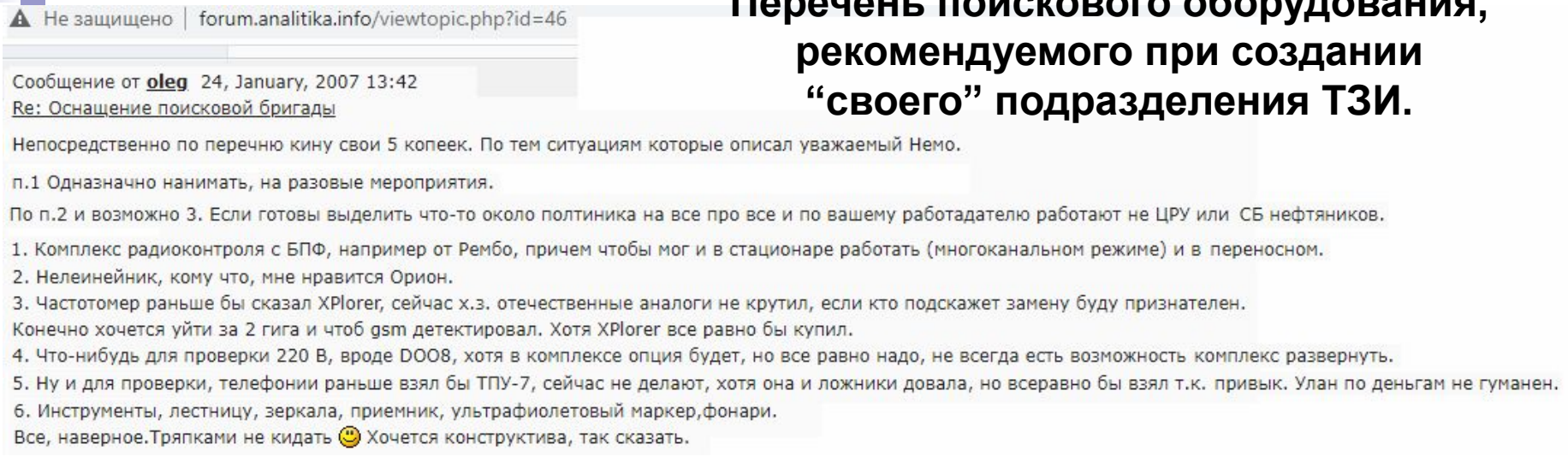
Или другой пример. Ядерные объекты не охраняют ЧОПы. Когда я служил, то спецсклад кто охранял? Совсем другие парни.

С искренним пожеланием успехов.

“Грамотные и сбалансированные СБ есть у очень немногих даже богатых контор” – в точку!

Ну и на счёт “*ума*” – ни убавить, ни прибавить: “**Бедные мы. Причём не материально. Средства у нас есть, а вот ума… Сложно? Да нет, всё просто. Как и во всём. Как исполнение ПДД**”

Перечень поискового оборудования, рекомендуемого при создании “своего” подразделения ТЗИ.



Не защищено | forum.analitika.info/viewtopic.php?id=46

Сообщение от **oleg** 24, January, 2007 13:42
Re: Оснащение поисковой бригады

Непосредственно по перечню кину свои 5 копеек. По тем ситуациям которые описал уважаемый Немо.

п.1 Однозначно нанимать, на разовые мероприятия.

По п.2 и возможно 3. Если готовы выделить что-то около полтиника на все про все и по вашему работадателю работают не ЦРУ или СБ нефтяников.

1. Комплекс радиоконтроля с БПФ, например от Рембо, причем чтобы мог и в стационаре работать (многоканальном режиме) и в переносном.
2. Нелеинейник, кому что, мне нравится Орион.
3. Частотомер раньше бы сказал XPlorer, сейчас х.з. отечественные аналоги не крутил, если кто подскажет замену буду признателен.
Конечно хочется уйти за 2 гига и чтоб gsm детектировал. Хотя XPlorer все равно бы купил.
4. Что-нибудь для проверки 220 В, вроде DOO8, хотя в комплексе опция будет, но все равно надо, не всегда есть возможность комплекс развернуть.
5. Ну и для проверки, телефонии раньше взял бы ТПУ-7, сейчас не делают, хотя она и ложники довала, но всеравно бы взял т.к. привык. Улан по деньгам не гуманен.
6. Инструменты, лестницу, зеркала, приемник, ультрафиолетовый маркер,фонари.
Все, наверное.Тряпками не кидать Хочется конструктива, так сказать.

“Замечание” по перечню предлагаемого оборудования – данное сообщение было в 2007 году *(см. дату)*, поэтому некоторые конкретные модели приборов, которые в нём упоминаются, на данный момент не актуальны.

В то же время, в нём совершенно верно перечислены “основные направления” поискового оборудования, которое должно быть в подразделении ТЗИ *(речь идёт о серьёзных компаниях, в которых есть реальная необходимость в такой работе и есть реальные специалисты, которые этим могут заниматься)*: комплекс радиоконтроля, нелинейный локатор, анализатор проводных линий *(как “силовых”, так и “слаботочных”)* и обязательно оборудование из п. 6. Нужно ещё добавить профессиональный обнаружитель видеокамер *(типа “**Оптик-2**”)*.

Хотелось бы обратить внимание на абсолютно верную фразу, касающуюся финансирования: **“Если готовы выделить что-то около полтинника на всё про всё …”** – т.е. 50 000 USD. Естественно, что когда речь заходит о такой сумме, то в нашей “молдавской действительности” *(да думаю, что не только в молдавской)* вопрос о приобретении поискового оборудования “автоматически снимается” в 99,9 % случаев.

Ещё раз об “оснащении поисковиков”.

Как было сказано ранее, когда речь идёт о поиске устройств съёма информации, то возможны два варианта: приглашение “человека со стороны” и работа “своими силами”. В обоих случаях эффективность поиска в первую очередь определяется подготовкой (профессионализмом) “поисковика” и его техническим оснащением.

Однако необходимо понимать, что уровень “технического оснащения” в каждом из этих случаев может принципиально отличаться.

Если говорить о “**приглашённом специалисте**” (естественно, речь идёт об официально работающих специалистах, имеющих соответствующую лицензию, а не о различного рода *“шаромыжниках”*), то он “по определению” **должен иметь в своём распоряжении весь набор поисковой техники**, позволяющий провести полноценную специальную проверку: нелинейный локатор, обнаружитель скрытых видеокамер, комплекс радиоконтроля, анализатор проводных линий, портативную рентгеновскую установку, оборудование для визуального осмотра помещения *(зеркала, эндоскоп, инструменты и т.д.)*. Образно говоря, “приходящий специалист” должен быть технически готов к проведению поисковых работ любой сложности.

Ещё раз об “оснащении поисковиков”.

Если же говорить о техническом оснащении “**своего**” **подразделения** по защите информации, то тут совсем другая ситуация – всё зависит от того, насколько серьёзно поставлена данная работа в конкретной компании, а если говорить “глобально”, то насколько такая работа вообще нужна для данной компании – учитывая, что “*компания компании рознь*”.

Как было отмечено в сообщении на форуме www.analitika.info: может быть небольшая фирма, где “… ***одному сотруднику поставили задачу – ищи! Что искать – сами пока не знают***.”, а может быть крупная компания, в которой “***всё по-взрослому***”. Кроме того, существует множество вариантов, когда речь идёт не о “юридических”, а о “физических” лицах, которые тоже хотят защитить свои секреты и пытаются что-то делать самостоятельно.

Естественно, что в большинстве случаев нет необходимости приобретать весь набор поисковой техники: *во-первых*, это будет нерентабельно, а *во-вторых* – для работы с поисковой техникой “в полном объёме” нужен специалист, который только этим будет заниматься.

Поэтому вопрос комплектации поисковой техникой “своего” подразделения ЗИ должен решаться “индивидуально” и “осознанно” в каждом конкретном случае.

Немного о “своём” подразделении защиты информации.

Если в компании принимается решение о создании “своего” подразделения защиты информации, то тут есть несколько важных моментов.

Необходимо помнить, что защита информации – это целый комплекс мероприятий, причём основную роль играют организационно-режимные меры.

Как было сказано ранее: техника “вторична” и с её покупкой спешить не стоит.

В первую очередь нужно **определиться с людьми *(человеком)***, **которые будут реально заниматься вопросами защиты информации**, и **обеспечить их начальную подготовку в этой области**.

Количество таких сотрудников будет зависеть от конкретной ситуации: в серьёзной компании может быть создано отдельное “штатное” подразделение, а в небольшой фирме это может быть один сотрудник, которому данные вопросы добавлены “в нагрузку” к его основным обязанностям.

Основной момент – это необходимость базовой подготовки данных сотрудников.

Как уже говорилось, к сожалению, на сегодняшний момент в Республике отсутствует система подготовки специалистов в области технической защиты информации для работы в “коммерческо-частном секторе” *(речь идёт о каких-либо учебных “курсах” по данному профилю)*.

Немного о “своём” подразделении защиты информации.

Обычно работодателю приходится принимать решение: отправлять своего сотрудника за рубеж на краткосрочные курсы по ТЗИ или пусть сотрудник “готовится самостоятельно” на месте *(“добывая” материал из интернета)* – естественно, что в 99% случаев выбирается второй вариант – *по этому поводу ранее было много очень хороших цитат с форума* www.analitika.info.

Ещё раз хочу подчеркнуть **принципиальный момент**: базовая подготовка сотрудников, которым будет поручено заниматься вопросами технической защиты информации, является обязательным условием – без этого нет смысла вообще “заморачиваться” на создание “своего” подразделения.

А далее всё уже зависит от конкретного человека – как было сказано на форуме: *“Ну а дальше развиваться, насколько ума хватает”*.

Что касается непосредственно подбора людей, которым будет поручено заниматься вопросами ТЗИ, то тут очень важно сделать правильный выбор, чтобы не “пролететь”: часто набирают людей, “имевших отношение к технике” – типа: “*он двадцать лет радиостанции и телефоны ремонтировал, так он и с защитой информации справится без проблем*” – не факт, что будет результат.

Как было сказано, всё будет зависеть от конкретного человека и от того “*насколько ему хватает ума, чтобы дальше развиваться*”.

Немного о “своём” подразделении защиты информации.

Правильный подбор людей для работы по линии ТЗИ это очень сложный и, я бы сказал, *“случайный”* процесс – имеется ввиду: “повезёт – не повезёт” *(естественно, что речь идёт о реальной работе, а не об её “имитации”)*.

Здесь ещё раз надо повторить, что защита информации – это целый комплекс мероприятий *(в том числе и не заметных на первый взгляд)*, основную роль в котором играют организационные меры.

А в представлении большинства “руководителей” и “начальников”, наоборот, всё сводится к *“проверкам”* и использованию т.н. *“глушилок”* – деятельность, которую *“начальство видит и оценивает”*.

Вот тут **очень важно**, чтобы сотрудник, отвечающий в компании за ТЗИ, мог довести до “руководства” реальное положение дел в этой области и предложить реальные грамотные решения.

Но очень часто те, кто отвечает в компании за ТЗИ, сами не знают что и как нужно делать, в результате чего вместо реальной работы происходит её “имитация” – главное, чтобы *“засветиться перед руководством”*.

Более того, иногда даже грамотные специалисты *(что уже редкость)* не хотят “разубеждать начальство” и, махнув на всё рукой, “плывут по течению”.

Пример бессмысленной (бестолковой) “*работы*” – зато “*начальство довольно*”!

Re: Про "Крону" бы послушать чего умного.
Пользователь: **serge331** (IP-адрес скрыт)
Дата: 31, October, 2006 00:49

Жил-был один очень подозрительный, но очень жадный человек. Но дела водил немалые. И чтобы не подслушал дел его кто-нить, задумал он им облом устроить. Решил проконсультироваться со специалистом. Но на хорошего денег жалко.Тогда вызвал он советника своего. Как крыша тот был незаменим, да и опер хороший, со связями. Но и он не без основания считал, что лучший детектор лжи - паяльник. Тот задачу воспринял, обратился к спецу, который числился у них "по технике". Тот долго не мудрствуя предложил несколько решений, но было выбрано одно- зашумить все нахрен. Затем все-таки уломали шефа на простенький радиоконтроль. Сказано - сделано. Дешево и сердито. Шеф доволен. Сам включает глушилку, когда "терки" серьезные, и руки потирает.
А на компьютере комплекса картинки разныя непонятные, приемник носится как оглашенный, оператор разгребает "ложники" потный, но сосредоточенный. Все на страже и в напряжении.
Красота одним словом.
С той стороны сначала приуныли, когда про такое коварство прознали. А потом заказали одному умельцу закладуху с прибамбасом. Да каким! Любо -дорого (в прямом смысле)! Включалась байда сама - когда шумовик запускали. Но могла и другими способами. А сигнал гнала ШПС под шумами. Немного, но под ними. Как вструмляли байду - песня отдельная. Но справились.
И жили они так долго, но не все счастливо.
И не нашли ее даже нелинейным локатором, при многочисленных обследованиях. Ведь в месте отклика слабенький сигнал второй гармоники уверенно "забивается" ржавыми скрутками, разложенными вокруг умелыми и добрыми руками.
А байда и по сей день стоит на месте, вот только не работает уже - батарейки сели. Но вложенные деньги отбила она многократно.

Вот такая грустная , но весьма поучительная история.

Re: Про "Крону" бы послушать чего умного.
Пользователь: **nemo** (IP-адрес скрыт)
Дата: 31, October, 2006 07:32

serge331 Написал:

> Вот такая грустная , но весьма поучительная
> история.

:) цинично, особенно про шумелку. Средства акустического зашумления - наш выбор!
Включать комплекс радиоконтроля при включенном широкополосном генераторе шума - а смысл?. Про то что ШПС под шумами совсем не видим - вам виднее, но например ШПС по сети 220 вольт шириной полосы 13 МГц мы научились выявлять (D-008 его не видит действительно) Нашлись там отличительные призаки. Разумеется никакие шумелки ВЧ использовать при радиоконтроле нельзя - теряется смысл. Но вы хотите сказать что если проводить долговременный контроль с накоплением - не вылезит эта ШПС в виде аномального превышения фона в проверяемом помещении по сравнению с опорной антенной (в помещении оператора например)?

История ваша говорит об одном - как обычно надо помнить что Защита Информации - комплекс ОРГАНИЗАЦИОННЫХ и технических мер.

Приходилось сталкиваться со *“специалистами”*, один из которых ежедневно *“проверял”* нелинейным локатором абсолютно “голую” бетонную стену в переговорной комнате – *правда, он прямо сказал, что просто создаёт видимость работы*, а другой во время совещаний сидел в соседнем помещении с анализатором спектра и *“сканировал эфир” – это в крупном офисном центре, где “со всех сторон” сотовые телефоны, Wi-Fi и т.д., за стеной от него вообще был холл, в котором постоянно находился десяток–другой посетителей, разговаривающих по мобильным телефонам и по сети Wi-Fi*.

Немного о “своём” подразделении защиты информации.

Вот так и бывает, что ситуация, связанная с сотрудником, отвечающим в компании за техническую защиту информации, складывается прямо как в песне Владимира Высоцкого:

И пощипывал он травку и нагуливал бока,
Не услышишь от него худого слова…
***Толку было с него**, правда, **как с козла молока**,*
Но вреда, однако, тоже никакого.

Знакомая ситуация? Вроде бы “у всех всё хорошо”: и человек вроде *“при деле”*, и “начальство довольно” – *“работа идёт”*. А “вред” как раз есть: начальство уверено, что “*граница на замке*” и *“можно спать спокойно”* (имеется ввиду, работать без каких-либо опасений) – там же *“специалист безопасность обеспечивает”* – а всё совсем наоборот…

Прямо как в рассказанной выше “грустной, но весьма поучительной истории”: *“И жили они так долго, но не все счастливо”* – нет, *“работник”* конечно же счастлив (“надувает щёки” и приличную зарплату получает), а вот у работодателя *(владельца компании)* могут быть проблемы...

Немного о “своём” подразделении защиты информации.

В то же время необходимо помнить, что известную поговорку: *“Заставь дурака богу молиться – он себе лоб расшибёт”* – никто не отменял.

Некоторая часть *“деятельных работников”* впадает в другую крайность – *иногда граничащую с “маразмом”* и от них можно ожидать чего угодно. Примерно как в фильме ***“Убойная сила”*** (серия *“Способный ученик”*), когда курсант-стажёр был искренне уверен, что в квартире спрятан труп – *которого вообще не было* – и чтобы его найти, решил самостоятельно провести там негласный осмотр *(для чего взял у криминалиста Семёна “прибор своей собственной разработки, реагирующий на трупный запах”)*, в результате чего:

“… *Полы в ванной, комнатах и коридоре вскрыты. Разрушена часть стены в спальне. Разбиты унитаз и раковина. Снесена декоративная колонна и часть подвесных потолков, принадлежащих соседям сверху. Повсеместно оторваны обои и везде натоптано*…”.

По этому поводу очень хорошо сказано в Уставе внутренней службы Вооружённых Сил СССР: “Военнослужащий обязан проявлять разумную инициативу” – ключевое слово “**разумную**” (от слова “**разум**”).

Немного о “своём” подразделении защиты информации.

Поэтому **хочу повторить ещё раз**: правильный подбор человека, который будет заниматься в компании вопросами технической защиты информации – это очень важный момент, к которому, к сожалению, часто относятся формально.

В ряде случаев, чтобы особо *“не заморачиваться”* с подбором сотрудника, вопросами ТЗИ поручают заниматься человеку, который имеет или раньше имел какое-то *“отношение к технике”* *(особенно, если такой человек сам будет настаивать на этом “назначении”)*.
А если этот *“работник”* ещё и искренне верит в то, что он *“реально специалист”*, тогда вообще “труба” *(для компании и работодателя)*.
Нет, конечно же возможно, что компании повезёт и такой человек окажется действительно толковым и адекватным работником.
Но, *на мой взгляд*, нынешние реалии больше соответствуют фразе:
“Раньше проводился тщательный подбор и отбор сотрудников, а сейчас идёт просто их набор”.

Такой *“специалист”* (кавычки!) фактически является ранее упоминавшимся героем **“Двенадцати стульев”** – *слесарем-интеллигентом Виктором Полесовым, который был уверен, что “знает и умеет всё” и периодически разворачивал бестолковую и бесполезную “бурную деятельность”*.

О техническом оснащении “своего” подразделения защиты информации.

Что касается непосредственно “оснащения” поисковым оборудованием, то здесь возможны различные варианты – всё зависит от конкретной ситуации.

Если речь идёт о крупной компании, в которой “всё по-взрослому” *(имеется ввиду, что там создано “штатное” подразделение по защите информации, набраны подготовленные специалисты, идёт необходимое финансирование, а **главное** – данная работа реально нужна компании)*, то здесь набор поискового оборудования может быть достаточно серьёзным – как минимум: нелинейный локатор, оптический обнаружитель видеокамер, комплекс радиоконтроля *(позволяющий вести круглосуточный контроль и анализировать “цифровые” сигналы – в том числе DECT, Wi-Fi, Bluetooth и т.д.)*, анализатор проводных линий и оборудование для визуального осмотра помещения *(досмотровые зеркала, эндоскоп, инструменты и т.д.)*.

Принципиальный момент: вся эта техника должна реально использоваться – *причём грамотно использоваться*, а не “лежать мёртвым грузом”. В противном случае нет смысла тратить деньги на её приобретение.

Хотя, как было сказано ранее, у нас в Республике компаний, в которых была бы серьёзно организована работа по технической защите информации, практически нет.

О техническом оснащении “своего” подразделения защиты информации.

Современная “молдавская действительность” такова, что в большинстве компаний, где пытаются что-то делать по линии ТЗИ, ситуация выглядит так: “**Одному сотруднику поставили задачу – ищи. Что искать – сами пока не знают**”. Естественно, что вопросы оснащения необходимым поисковым оборудованием практически не решаются – как правило, всё сводится к покупке на www.999.md каких-либо дешёвых *“чудо-приборов”* из *“клоунского набора”*, которые годятся только для “самообмана” и “самоуспокоения” *(примеры см. далее)*.

Необходимо отметить, что финансирование вопросов ТЗИ, как правило, носит “разовый” характер: если удаётся **с большим трудом** убедить руководство компании на выделение какой-либо суммы, то это обычно только один раз. Поэтому очень важно, чтобы эти деньги были использованы грамотно и эффективно, а не были потрачены на бесполезную ерунду.

Как правило, на приобретение поисковой техники можно “с трудом получить” **максимум 2000 – 3000 USD** – причём большинство работодателей уверены, что за эти деньги можно купить *“обнаружитель всего”*.

Понятно, что ни о каком “полноценном оснащении” поисковым оборудованием за такие деньги не может быть и речи, в то же время даже эту сумму можно использовать достаточно эффективно.

Пример *“универсального детектора”* для обнаружения подслушивающих устройств, предлагаемого на “молдавском рынке” – как говорится: *было бы смешно, если бы не было так грустно*...

Очень *“сильна”* фраза: “*обнаруживает излучение GPS*” – наверное, речь идёт о том “*излучении*”, которое исходит прямо от спутников…

Ну а это – вообще “шедевр”: *“позволяет со 100% вероятностью определить, прослушивается ли ваш мобильный или стационарный телефон”*.

И думаю, что в ФБР, ЦРУ и особенно в Моссад очень бы удивились, если бы прочитали это объявление и узнали из него, что у них используют это “чудо техники”.

Ещё один *пример “высоких технологий”* (кавычки!) для обнаружения подслушивающих устройств, предлагаемый на “молдавском рынке”.

www.999.md/549238

999

подать объявление | интернет магазин | каталог компаний

Главная ▾ | Все остальное | Охрана и безопасность | ДЕТЕКТОР ЖУЧКОВ, ПОДСЛУШИВАЮЩИХ УСТРОЙСТВ,

ДЕТЕКТОР ЖУЧКОВ, ПОДСЛУШИВАЮЩИХ УСТРОЙСТВ, ВИДЕОКАМЕР

автор: sasa дата: 07 ноября 2012, 14:56 регион: Кишинёв мун. тип: Продам просмотров: 13

Проверте ваш кабинет или дом или машину на прослушку.

Видит проводные камеры, беспроводные и все типы жучков, радиотелефоны и мобильные телефоны, абсолютно все передающие устройства.

- Размеры 93 x 48 x 17 мм.
- Вес 58 гр.
- Диапазон обнаружения радиозакладок 1МГц - 6,5ГГц.
- Время работы: обнаружение видео оптики - 6 часов, радиосканирование - 14 часов.
- Режим работы: звуковой и вибрация.
- Питание: встроенный аккумулятор 450 мАч.
- Условия работы: -20 + 50 град, влажность от 10 до 90 %.

В комплекте : детектор, наушники, зарядка

Цена 500 лей

Так как остался 1 отдам за 470 лей

регион: **Кишинёв мун.** контакты : +373

О техническом оснащении “своего” подразделения защиты информации.

При выборе поискового оборудования нужно отталкиваться от того, кто реально будет работать с этой техникой.

Как уже говорилось: одно дело если в компании создано “штатное” подразделение по защите информации, укомплектованное грамотными специалистами, которые прошли соответствующую подготовку и у которых есть необходимые “знания, умения и навыки” по работе с поисковым оборудованием *(речь идёт о таком оборудовании, как комплекс радиоконтроля, анализатор проводных линий, нелинейный локатор – для грамотной работы с которыми нужно понимание происходящих физических процессов)* и совсем другое дело если “поисковыми вопросами” в компании занимается всего один человек – как правило, кто-то из “личников”, на которого данная деятельность возложена в качестве “нагрузки”.

Учитывая, что второй вариант наиболее характерен для молдавских компаний, **основное внимание акцентируем именно на нём**:
задача *“поиска возможно установленных устройств съёма информации”* поручена сотруднику личной охраны *(как правило, бывший “силовик”)*, который не имеет какой-либо специальной подготовки в области защиты информации.

Типовая ситуация, с которой сталкиваются многие сотрудники личной охраны.

Автор	Сообщение
Ridick_777 Участник OFF 123456789 OVER с мар 2010 Санкт-Петербург Сообщений: 11	Дата: 18 Мар 2010 01:48:43 # Привет Братцы! Хотя я и новичок в деле безопасности ТКУИ, но домашнюю работу выполнил хорошо, профессия у меня такая, быть подготовленным. :) Отлично понимаю, что для защиты стационарного объекта применяеться радиомониторинг с анализатором спектра, ибо все остальное не серезно. не считая нелинейные локаторы, комплексы итд. работа у меня мобилная. как собачке бегать за ОЛ, поэтому non-linear junction уш точно не подходит и по размеру, и по временным затратам и по $$$. Сначала (наевшись рекламы) хотел покупать Скорпион, потом кто то посоветовал Xplorer. Ясно, что device должны быть портативнами, идеально один, на крайняк два. Основной канал радиоканал, ибо как с другими боротся (или точнее - затруднять; избегать) - более менее ясно. Конечно. задачи нет найти цифровую или обойти федералов.
G305e Участник OFF 123456789 OVER с июл 2007 Оттуда Сообщений: 1919	Дата: 21 Мар 2010 03:51:04 # **Ridick_777** без обид - сочувствую вашему нанимателю. Скачете с одного на другое, не понимая сути вопроса. Вы с Питера - сходите в Бэтмэн, купите нашу книгу http://www.batman.ru/e-store/literature/index.php?SECTION_ID=970&ELEMENT_ID=11065 Для понимания что же сейчас используют - достаточно. Вы себе представляете что значит поставить закладку на 10 ГГц, и как там распространяются радиоволны? Никто не будет для комерсантов и простых чинуш лепить такое. *если я ошибаюсь про video-hunter, пожалуйста, скорректируйте меня* не более чем за 10 секунд найдёт включенную беспроводную камеру в вашем помещении. Стандартный хантер ловит до 2600 МГц, новое поколение за 5.8 ГГц шагнуло (китайцы начали клепать там камеры, вот и хантеры пришлось делать новые). Но только видео(!) поймает *акустического радиоканала: любительского и професионального. Как стационарно, так и на выездах.* если быть максималистом - при проф угрозах без круглосуточного непрерывного радиоконтроля сейчас нечего делать. *Не думаю, что на этом форуме большинство смогло бы обойти федеральные мероприятия или найти digital bug. (че ни так - поправляйте).* при наличии соответствующего оборудования - тот кто умеет - найдёт. *Думаю, Теоретически digital можно просечь локатором, правда в реали они у банков, и у состоятельный предпринимателей (у СБ). Ну, а с двумя гармониками - просто мечта. :))) Поработать бы с таким.* нелинейный локатор может найти многое, но не всё. Если говорить и дальше о страшилках, то поищите поиском в сети информацию о "оптический микрофон COM"
Fath Участник OFF 123456789 OVER с мая 2007 Ярославль Сообщений: 2320	Дата: 21 Мар 2010 11:40:45 # **Ridick_777** *Легко сказать - определитесь. Откуда мне знать кому в голову придет "обзавестись" наблюдением? Тупому скинхеду или организованным, дисциплинированным специалистам? Ок, мне за это деньги платят, и слава Богу, с мозгами миловал.* Мдя, тут невольно вспоминается поговорка: "Скупой платит дважды" (я про Вашего работодателя). Не обижайтесь, но Вы не знаете даже элементарных основ того, чем пытаетесь заниматься, а без знаний и опыта в этом деле никакая техника не поможет, тут надо учиться, учиться и учиться. Причём помимо овладения базовыми основами крайне желательно пройти бы специальное обучение, которое хоть и будет стоить немалых денег, но после него вы хотя бы будете иметь некоторое представление о потенциальных угрозах и о том, что, где и как искать. Прийти и с умным видом помахать по комнате приёмником, после чего заявить, что всё нормально, тоже конечно можно, но если потом что-то "уплывёт", то ответственность-то ляжет на Вас.
Ridick_777 Участник OFF 123456789 OVER	Дата: 22 Мар 2010 14:08:44 # Спасибо за замечания. Клиенты о подготовке (или ее отсутсвии) знают, врать не стал. Поэтому жалеть здесь не кого.

Типичная ситуация…

Предыдущий слайд реально отражает типовую ситуацию, когда вопросами защиты информации *(в частности, поиском устройств съёма информации)* поручено заниматься сотруднику “лички”.

Очень типична фраза “личника”, касающаяся выбора поискового оборудования: “*Сначала (наевшись рекламы) хотел покупать …, потом кто-то посоветовал …*” (именно так очень часто и происходит выбор – *“наевшись рекламы”*).

Абсолютно правильны и фразы, которые звучат в ответ:
“*Без обид – скачете с одного на другое, не понимая сути вопроса*” и
“*Не обижайтесь, но Вы не знаете даже элементарных основ того, чем пытаетесь заниматься. А без знаний и опыта в этом деле никакая техника не поможет – тут надо учиться, учиться и учиться*”.

Причём всё сказанное относится не только к “личникам”, но и ко всем “неспециалистам”, кому поручили заниматься вопросами ЗИ “в нагрузку”:
это и *“айтишник”*, и *“связист, который 20 лет радиостанции ремонтировал”*, и *“просто хороший парень, которому шеф доверяет”*.

“Самообразование” имеет свои пределы.

Так что ещё раз хочется повторить фразу: *“Без знаний и опыта в этом деле никакая техника не поможет – тут надо учиться, учиться и учиться”*.

Конечно же идеальный вариант – это обучение на специализированных курсах. Но в современной “молдавской реальности” практически всем, кому поручено заниматься вопросами поиска устройств съёма информации, приходится “учиться” самостоятельно – как было очень хорошо сказано на форуме: *“насколько ума хватает”*.

В то же время **нужно чётко понимать**, что для настоящей работы с некоторыми видами поискового оборудования кроме прохождения кратковременных “профильных” курсов необходимо иметь базовое техническое образование.

Например, для **реальной** работы с комплексом радиоконтроля у оператора должно быть как минимум среднее радиотехническое образование и он должен знать и понимать как теорию электромагнитного поля и распространения радиоволн, так и принципы работы современных систем беспроводной связи и ***ещё много чего***. А для работы с серьёзным анализатором проводных линий *(типа **TALAN**)* оператор должен знать не только принципы построения и особенности работы кабельных сетей разных типов, но и протоколы цифровых АТС и VoIP-систем.

Визуальный осмотр – основной метод поиска *(моё личное мнение)*.

Моё личное мнение: сотрудник личной охраны, для которого **основная задача – обеспечение жизни** и **здоровья охраняемого лица**, никогда не сможет освоить все нюансы работы с такого рода оборудованием, как *комплекс радиоконтроля, анализатор проводных линий и т.п.* – этим должен заниматься отдельный человек *(которого обычно нет)*, имеющий соответствующее образование и подготовку.

В то же время **нужно чётко понимать и постоянно помнить**, что все активно рекламируемые и продаваемые *“обнаружители всех видов жучков”*, которые *“не требуют какой-либо специальной подготовки пользователя”* и *“работают”* по принципу *“пищит – не пищит”* – это чистый “развод”.

Поэтому **основной метод** поиска устройств съёма информации, на который должен делать упор “личник”, отвечающий за вопросы защиты информации, – это **тщательный визуальный осмотр** проверяемого помещения.

Моё личное мнение: *визуальный осмотр (специальное обследование) помещения вообще является самым важным элементом поисковых работ и имеет приоритет над “чисто технической” специальной проверкой – по крайней мере, когда речь идёт о “коммерческо-частном секторе”.*

Хотя конечно же для обнаружения некоторых устройств съёма информации без использования технических средств поиска не обойтись.

Визуальный осмотр – основной метод поиска.

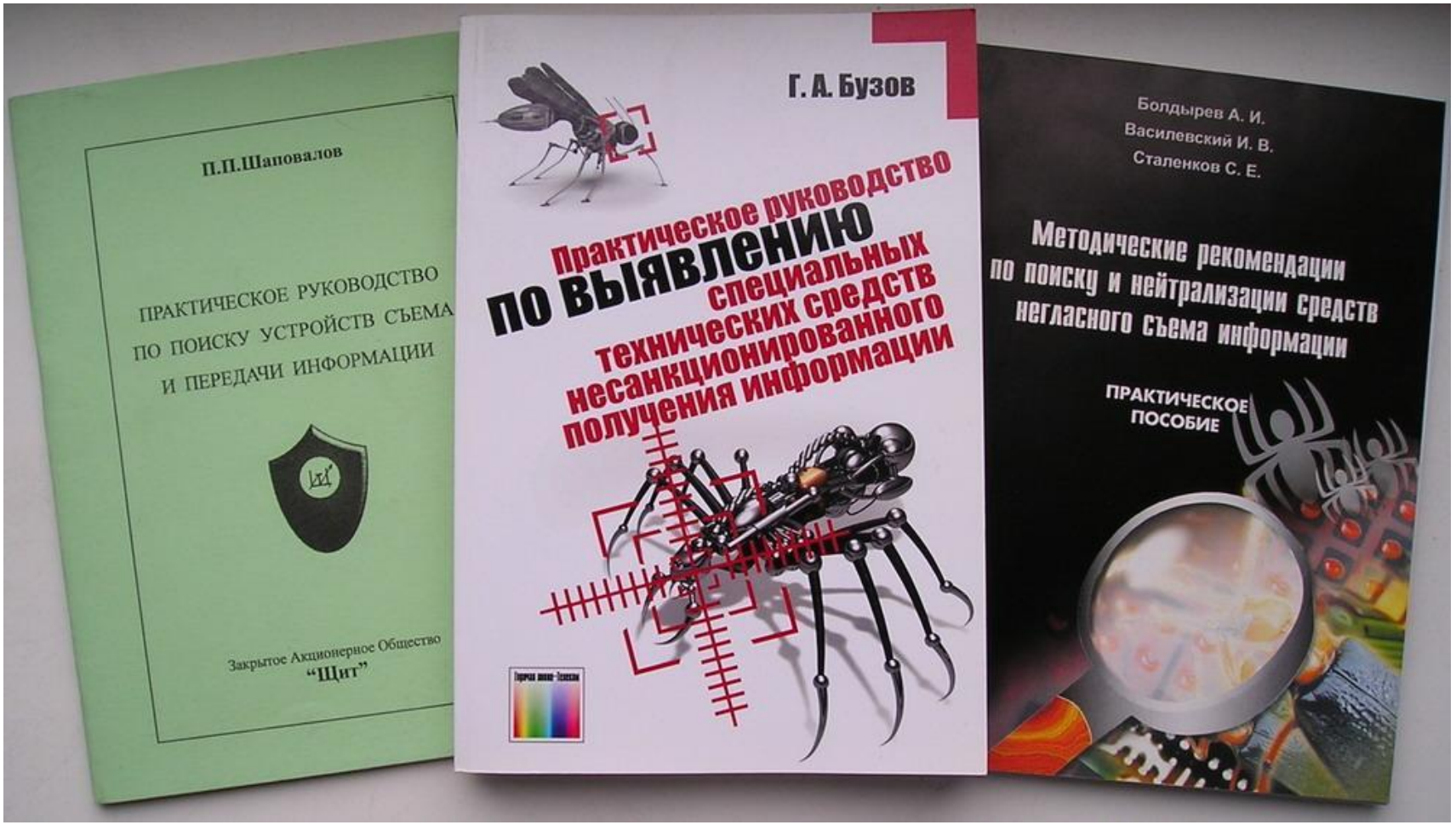
Естественно, что визуальный осмотр помещения должен проводиться очень тщательно и “системно” – чтобы ничего не пропустить.
Вариант “пятиминутного” осмотра, проводимого кое-как, даже не обсуждается – это просто “имитация работы”.

При проведении визуального осмотра помещения с целью поиска возможных устройств съёма информации **будут очень полезны знания и навыки из “смежных областей”, которые могут иметься у “личников”** – например, инженерно-сапёрная подготовка *(для бывших “армейцев”)* или опыт проведения обысков и осмотра места происшествия *(для бывших сотрудников правоохранительных органов)*.

Адекватный и **думающий** человек, освоивший методику визуального осмотра помещения, может обнаружить большинство устройств съёма информации, которые используются в “коммерческо-частном секторе” *(за исключением вариантов “**глубокого камуфляжа**”)*.

Примечание: под “**глубоким камуфляжем**” я имею ввиду как установку средств съёма информации в элементах конструкции здания, требующую проведения каких-либо строительно-монтажных работ – *например, “штробление” стен с последующим “замуровыванием” в них закладных устройств*, так и использование закладных устройств, которые “заводским способом” установлены внутри каких-либо предметов интерьера.

Методические материалы по поиску устройств съёма информации.



Имеется достаточно большое количество литературы, посвящённой вопросам поиска устройств съёма информации, на базе которой можно разработать “свою” методику *(инструкцию)* проведения визуального осмотра помещения.

Методика проведения визуального осмотра помещения должна быть “оформлена” отдельным документом *(инструкцией)*, в котором чётко и ясно указывается “пошаговый” порядок действий.

Ещё раз о необходимости “комплексного подхода” к вопросам ЗИ.

Необходимо постоянно помнить, что “поисковые мероприятия” являются только одной из составляющих *(причём не основной)* целого комплекса мер, направленных на обеспечение защиты информации.

Сотрудник, отвечающий за их проведение, не может быть “зациклен” только на поиске – он должен понимать проблему “в целом” и решать её комплексно *(нужно отметить, что очень часто здесь не всё так просто получается)*.

Кроме того, для проведения качественного осмотра помещения необходимо взаимодействие с другими работниками фирмы.

Поэтому очень важно, чтобы при возникновении каких-либо вопросов у “личника” была возможность оперативно обсудить их как со своим руководством *(с начальником СБ или непосредственно с ОЛ)*, так и с сотрудниками компании, взаимодействие с которыми может понадобиться *(с секретарём, с водителем “шефа”, с системным администратором и т.д.)*, чтобы скоординировать необходимые действия, связанные с осмотром.

Вроде бы это элементарные истины, про которые и говорить не стоит, но на практике такое “взаимодействие” часто отсутствует – по разным причинам: иногда сотрудник личной охраны *“боится слово сказать перед начальством”*, иногда просто *“тормозит”*, иногда *“конфликтует”* с другими работниками и т.д.

Очень важный момент – составление “модели нарушителя”.

G305e
Участник

Дата: 19 Мар 2010 08:50:34 #

http://www.radioscanner.ru/forum/topic41066-1.html

Вы уж определитесь, чего боитесь, а то так мы и до космической связи и перехвата ЗАС дойдём.

Ridick_777
Участник

Дата: 21 Мар 2010 01:31:18

Легко сказать - определитесь. Откуда мне знать кому в голову придет "обзавестись" наблюдением?
Тупому скинхеду или организованным, дисциплинированным специалистам? Ок, мне за это деньги платят, и слава Богу, с мозгами миловал.

Выше приведена типичная ситуация: сотрудник “лички”, которому поручено заниматься вопросами защиты информации, пытается определиться с возможными угрозами.

Разработка “**модели нарушителя**” (составление “перечня возможных угроз”) является **основой** для проведения работ по защите информации в целом и поиску устройств съёма информации в частности.

В “классическом” варианте для составления “модели нарушителя” используются специальные методики, в которых учитывается очень много факторов, влияющих на итоговый результат, а обработка исходных данных идёт в том числе с использованием математического моделирования. Но такой вариант подходит только для компаний, в которых “всё по-взрослому” – где есть **реально** работающее подразделение по защите информации, укомплектованное **грамотными подготовленными** специалистами.

Необходимо чётко понимать, что в разработке “полноценной” модели нарушителя должны участвовать не только “профильные” специалисты, работающие по линии ТЗИ, но и сотрудники других подразделений службы безопасности компании – в том числе и руководитель службы безопасности.

Очень важный момент – составление “модели нарушителя”.

В то же время, в абсолютном большинстве случаев, когда вопросами ТЗИ поручено заниматься “по совместительству” кому-нибудь из сотрудников компании, не имеющих специальной подготовки в области защиты информации: *например, одному из “личников”, технику охранных систем (система ОПС и т.п.) или связисту, который 20 лет радиостанции и телефоны ремонтировал* – вообще нет смысла “заморачиваться” на классические методики разработки модели нарушителя – они в них просто ничего не поймут *(не хочу никого обидеть)*.

Разработка **полноценной модели нарушителя** – очень важный момент, но это тема отдельного серьёзного разговора, при этом у слушателей должны быть базовые знания по целому ряду общеобразовательных и специальных дисциплин. Поэтому в данной презентации этот вопрос рассматриваться не будет – как говорится в таких случаях: “*Замнём для ясности*”.

В случае типовой “молдавской действительности” (*когда заниматься поиском средств съёма информации поручено “в нагрузку” одному из сотрудников личной охраны, не имеющему полноценной специальной подготовки*) можно использовать “упрощённый вариант” оценки возможных угроз – далее приведены некоторые рекомендации по этому поводу (*достаточно простые, но надеюсь, что полезные*).

Примечание: *нужно помнить, что **основная угроза** – это “человеческий фактор”, и бороться с ней намного сложнее, чем с “техническими” угрозами*.

Очень важный момент – составление “модели нарушителя”.

Основная цель разработки модели нарушителя – правильно определить **реальные** угрозы, чтобы принять соответствующие меры для их выявления и “блокирования”.

При этом необходимо помнить, что технические каналы утечки информации могут быть как искусственными *(специально созданными злоумышленником)* – например, установка в нужном помещении устройств съёма информации, так и естественными – которые существуют “сами по себе” (*плохая звукоизоляция, открытое окно и т.д.*).

Соответственно будут различные способы “борьбы”: что-то можно “обнаружить и изъять”, а что-то “существует по определению” и его можно только “заблокировать или устранить”.

Очень важный момент: в каждом конкретном случае **нужно определить наиболее реальные угрозы и бороться в первую очередь именно с ними**.

Очень часто, из-за неправильной оценки угроз, идёт “война с ветряными мельницами”, а реальные угрозы остаются незамеченными, например:

- Периодически с помощью детектора поля *“ищут радиозакладки”*, но при этом не понимают, что 90% радиопередающих устройств, которые на сегодняшний день представляют реальную угрозу *(передатчики на базе GSM, Wi-Fi или Bluetooth)*, будут “не активны” в момент такой *“проверки”*.
- Помещение периодически проверяют на наличие скрытых видеокамер, но при этом окна постоянно не зашторены и с наружи всё просматривается как “в телевизоре” *(особенно когда включён свет)* и для наблюдения за вами злоумышленнику вообще не надо что-то “устанавливать” в помещении.
- Для борьбы с гипотетическим *“лазерным съёмом”* устанавливают виброакустическую защиту на окна *(только на них)*, но при этом абсолютно не обращают внимание на реально существующие “акустоводы” (система вентиляции и т.п.), по которым действительно возможна утечка информации.

Поэтому правильная оценка угроз – это принципиальный момент для **реальной** ЗИ.

“Кто в доме хозяин?” – от этого много зависит...

Если рассматривать помещения **с точки зрения “собственности”** – *кто “хозяин данной территории” и кто выступает в роли возможного “злоумышленника”, который имеет определённую “свободу действий” по установке средств съёма информации на данной территории* – то здесь **возможны три основных варианта**:

- Это ваше помещение – т.е. **вы находитесь на “своей территории”**, а посторонние лица не могут *(точнее сказать – “не должны”)* бесконтрольно попасть на неё.
- Это **“чужая территория”** *(чужой офис, гостиница, “баня” и т.д.)* и **в качестве злоумышленника выступает непосредственно её хозяин**, который свободно может проводить на ней “любые работы”.
- Это **“чужая территория”**, но **в качестве злоумышленника выступает** не её хозяин, а **“третье лицо”**, которое имеет туда постоянный или периодический доступ, но с “ограниченными возможностями” по проведению каких-либо действий – например, *“постоянный посетитель”* или кто-то из работающего там персонала.

В каждом из этих случаев будут свои наиболее вероятные угрозы в плане того, что именно может быть использовано злоумышленником.

“Своя территория”.

В этом случае всё зависит в первую очередь от того, как на объекте выполняются **организационно-режимные мероприятия**, которые являются **основой всего**.

Если на вашем объекте “полный бардак” и “проходной двор”, то возможны самые различные “варианты” – хотя даже в этом случае достаточно мала вероятность “штробления” стен, полов или потолков.

Если же на объекте правильно организованы режимные мероприятия, то возможности потенциального злоумышленника значительно снижаются.

Принципиальный момент: любые организационно-режимные мероприятия должны выполняться **реально**, а не формально. Например, если на объекте ведётся круглосуточное видеонаблюдение, но никто ежедневно не просматривает записи – не будет никакого толка. То же самое касается охранника, который *“сопровождает”* работы по сборке мебели в кабинете руководителя или ремонту кондиционера в комнате для переговоров – при этом он стоит рядом с рабочими, но не наблюдает за ними, а *“висит”* в своём смартфоне.

Нужно чётко понимать, что грамотно организованные и правильно выполняемые режимные мероприятия важнее и эффективнее чисто технических мер по защите информации – *моё личное мнение*.

“Своя территория”.

Если вы находитесь на “своей территории”, то прежде всего необходимо оценить **реальные возможности** потенциального “злоумышленника” *(составить “модель нарушителя”)*.

По “тактике” применения средств съёма информации можно выделить три основные группы: **заранее внедряемые** (в том числе с “глубоким камуфляжем”), **вносимые** (“заносные”) и “**беззаходовые**”.

Очень **важно правильно оценить, кто непосредственно будет “внедрять” (“заносить”) данные устройства на ваш объект** – здесь всё зависит в большей степени не от “технических”, а от “административных” возможностей злоумышленника: одно дело если “закладка” была установлена в ходе *“тайного проникновения в помещение” (как показывают в кино)*, её внедрили *“проводившие ремонт кондиционера рабочие”* или её оставил приходивший посетитель и совсем другое дело если у вас работает человек, который может свободно устанавливать “закладку” в нужном помещении и забирать её.

От этого во многом зависит, какие именно средства съёма информации использует злоумышленник – *например, при наличии в вашем окружении “засланного казачка” наиболее вероятно использование им миниатюрных цифровых диктофонов, которые очень сложно обнаружить*.

“Своя территория”.

Заранее внедряемые средства съёма информации рассчитаны на долговременную работу и, как правило, они имеют сетевое электропитание или “очень электроёмкое” автономное питание и высокий уровень камуфляжа. Такие устройства обычно устанавливаются в ограждающие конструкции помещения, в элементы мебели *(именно “встроены” в мебель, а не просто “положены” в неё)*, в электророзетки, осветительные приборы, распределительные коробки *(“дозы”)*, в элементы слаботочных систем *(в датчиках системы ОПС и т.п.)* или в бытовую электронику *(кондиционер, телевизор, оргтехника и т.п.)*.

В большинстве случаев передача информации осуществляется по радиоканалу – *в том числе по сети сотовой связи или Wi-Fi* , а так же по “штатным” проводным линиям, выходящим из помещения *(электросеть или слаботочные линии)*. *Теоретически возможна и прокладка специальных проводных линий, но для “коммерческого злоумышленника” это маловероятно*.

Для установки *(внедрения)* таких средств съёма информации злоумышленнику необходимо “свободно работать” в нужном помещении достаточно длительное время или эти устройства должны быть “внедрены” в мебель или в бытовую технику ещё до того, как их привезут к вам.

Поэтому ещё раз: **организационно-режимные мероприятия – это главное**!

“Своя территория”.

Вносимые (**“заносные”**) средства съёма информации как правило имеют автономное питание и, соответственно, ограниченное время работы – от нескольких часов до нескольких месяцев.

Данные устройства могут быть выполнены в виде отдельных модулей или могут быть закамуфлированы под различные бытовые предметы: кусок картона, деревянный брусок *(плитка паркета)*, ручка *(маркер)*, пепельница, калькулятор, папка для бумаг, книга, детская игрушка, пульт ДУ, банковская карта и т.д.

Принципиально существует два типа “заносных” средств съёма информации: **работающие в режиме** “**накопителя**” (диктофоны и видеорегистраторы) и **работающие в режиме** “**радиопередатчика**” (аудио- и видео) – в том числе используя для передачи информации сеть сотовой связи, Wi-Fi, Bluetooth и т.д.

Соответственно, есть определённые “нюансы” относительно возможных мест установки “заносных” средств съёма информации. Если злоумышленник использует какой-либо “накопитель”, то он обязательно должен установить его так, чтобы была возможность быстрого доступа к данному изделию для периодического съёма накопленной информации. Если же злоумышленник использует “радиопередатчик” и не собирается потом изымать его или периодически менять в нём элементы питания (вариант *“бросового”* радиомикрофона, который *“отработает и умрёт”* на объекте), то такое изделие может быть “глубоко запихано” в самые труднодоступные места.

“Своя территория”.

Некоторые **вносимые** (**“заносные”**) средства съёма информации могут иметь питание от электросети – например, если они встроены в “тройник”, электроудлинитель, электролампочку, блок питания для ноутбука или зарядное устройство для мобильного телефона и т.д., а так же от слаботочных источников *(в том числе от “штатных” USB-портов)* – например, если они установлены в датчиках охранно-пожарной сигнализации (ОПС), выполнены в виде “флэшки”, встроены в “мышь” или в USB-кабель и т.д. В этом случае время их работы будет практически не ограничено, а информацию они или накапливают на съёмную карту памяти или передают по радиоканалу – как правило, по сети сотовой связи или Wi-Fi.

Что касается “заносных” средств съёма информации, которые имеют питание от электросети, то в 99 % случаев “злоумышленник” не будет тратить время и “вставлять” их в “нужный корпус” *(в электроудлинитель, “тройник” и т.д.)* в самом помещении *(моё личное мнение)* – он просто заменит ваш “электроприбор” на такой же, но предварительно “доработанный”.

“Своя территория”.

В настоящее время **вносимые** (**“заносные”**) средства съёма информации наиболее часто используются злоумышленниками в “коммерческо-частном секторе”. Это связано как с относительной доступностью таких устройств – например, миниатюрные диктофоны и некоторые модели видеорегистраторов продаются совершенно свободно, так и с относительной “простотой” их установки и достаточно низкой ценой.

Для установки (“заноса”) таких средств съёма информации злоумышленнику необходимо попасть в нужное помещение на достаточно короткое время – иногда “на всё про всё” потребуется меньше минуты *(естественно, если злоумышленник подготовлен в этом плане)*.

Особо нужно отметить, что сейчас в свободной продаже – *например, в различных “интернет-магазинах”* – имеется большое количество высокотехнологичных устройств, которые позиционируются производителями как *“охранные системы”*, но могут быть использованы злоумышленниками как средства съёма информации: в частности, речь идёт о системах видеонаблюдения, закамуфлированных в “умных лампах” или в различных бытовых предметах.

Так что опять о главном: “**Учёт плюс контроль**” – т.е. **режим**!

Некоторые примеры “заносных” средств съёма информации – см. далее.

“Поисковик” обязан досконально знать “свою территорию”.

Что касается поисковых работ на “своей территории”, то у сотрудника, отвечающего за их проведение, всегда должно быть “преимущество своего поля”.

Есть такая хорошая фраза: *“Знай и люби свой город!”* – как ни странно, она абсолютно подходит и под работу “поисковика” – конечно же “любить” свою компанию не обязательно *(достаточно быть просто лояльным к ней)*, но досконально “знать” помещения компании, в которых проводятся проверки *(кабинет руководителя, комната отдыха, переговорная комната и т.д.)*, данный сотрудник **обязан**.

Нужно знать не только все возможные места, в которых могут быть установлены устройства съёма информации, но и все “элементы обстановки” помещений *(предметы интерьера, книги, канцелярские принадлежности и т.д.)*. Понятно, что “за один день” этого не узнаешь и не запомнишь – это должна быть системная работа, которая ведётся планомерно и постоянно.

Здесь очень важно взаимодействие с другими сотрудниками компании – *секретарём, системным администратором, “хозяйственником” и т.д.*, которые должны немедленно информировать как о всех “изменениях обстановки”: *новая мебель или бытовая техника, подарки и т.д.*, так и о всех проводимых работах: *ремонт чего-либо, осмотр кондиционера, проверка отопления и т.п.*

“Поисковик” обязан досконально знать “свою территорию”.

Как было сказано, “изучение своей территории” – это планомерная и “системная” работа, которую нужно вести постоянно.
Естественно, что в случае “штатного” подразделения по защите информации данная работа ведётся штатным сотрудником в “плановом порядке”.
Совсем другое дело, когда речь идёт о “личнике”, на которого вопросы ЗИ возложены в качестве “нагрузки” в дополнение к его основным обязанностям, – он целыми днями “мотается” с ОЛ и ему без этого проблем хватает.
Но тут ничего не поделаешь – это принципиальный момент с точки зрения ЗИ.

Для изучения “конструктивных особенностей” помещения целесообразно не только самостоятельно его “исследовать” в поиске возможных “нычек”, но и не стесняться задавать вопросы “профильным специалистам”, которые его обслуживают: электрику, сантехнику, администратору (“хозяйственнику”) и т.д.
В результате такого *“изучения местности”* сотрудник, отвечающий за вопросы защиты информации, должен знать все возможные “потайные места”: щели и полости в дверной коробке, прикрытые наличниками; конструктивные полости в мебели, которая установлена в помещениях; пустоты в подоконнике, закрытые торцевой крышкой; различные “нычки” в диванах и креслах; кабель-каналы, проложенные в полу; ситуацию с плинтусами; электрические “дозы” и т.д.

Поиск различных “нычек”, которые могут быть в помещении.

В каждом помещении есть различные “нычки”, в которых могут быть спрятаны средства съёма информации. Причём располагаться они могут в самых различных местах – *один из элементарных вариантов приведён на фото*.

“Поисковик” обязан знать все такие места на “своей территории”, а при проведении осмотра на “чужой территории” – **думать** и находить их.

“Учёт и контроль” – обязательная составляющая поисковых работ.

Для контроля за “элементами обстановки помещения” целесообразно вести их строгий “учёт”: очень полезно составить перечень **всех** предметов, находящихся в помещении *(т.н. “паспорт объекта”)* – чтобы при каждой проверке производить соответствующую “сверку”. Но в реальности это делают только там, где с вопросами защиты информации “всё по-взрослому”, а в большинстве случаев на это “не заморачиваются”.

Как минимум нужно “вести учёт” тех предметов, которые могут иметь “штатное” электропитание *(как “силовое” или “слаботочное”, так и “батарейное”)*: электроудлинители и “тройники”, зарядные устройства и блоки питания для телекоммуникационных устройств и бытовой техники, телефонные аппараты, датчики ОПС и различных технологических систем *(система типа “умный дом”)*, калькуляторы, электрические часы *(настольные и настенные)*, пульты ДУ и т.д. Как было сказано ранее, в 99% случаев злоумышленник не будет тратить время на “внедрение” устройств съёма информации в ваш предмет интерьера, имеющий “штатное” электропитание – *для этого он должен достаточно длительное время свободно “работать” в вашем помещении* – он просто заменит этот предмет на такой же, но предварительно “доработанный”, что займёт у него считанные секунды *(конечно, при соответствующей подготовке)*.

“Учёт и контроль” – обязательная составляющая поисковых работ.

Самый простой вариант “учёта” предметов интерьера – это составление их списка с указанием наименований и заводских *(серийных)* номеров, которые указаны на большинстве таких устройств *(практически на всех калькуляторах, зарядных устройствах, блоках питания, датчиках, на многих пультах ДУ и т.д.)*.

В большинстве случаев серийный номер изделия указан “где-то сзади” мелким шрифтом и его так сразу не увидишь. Как было сказано ранее, злоумышленник может заменить ваше устройство на точно такое же, но “доработанное” – в то же время, “выбить нужный серийный номер” на нём практически не возможно *(по крайней мере, если речь идёт о “коммерческо-частном секторе”)*.

На некоторых изделиях серийного номера может не быть вообще – например, на электроудлинителях, “тройниках” и т.д. – в этом случае нужно разработать “свою систему меток”, которая выглядит естественно и не бросается в глаза: например, с помощью царапин, пятен и т.п.

В “классическом варианте” для этого используется специальный маркер, метка от которого видна только при ультрафиолетовом освещении. Однако для молдавского “коммерческо-частного сектора” такое маркирование большая редкость *(хотя УФ-маркер и УФ-фонарь стоят практически “копейки”)*.

Естественно, что перед “маркированием” нужно убедиться, что данное изделие не содержит в себе каких-либо посторонних “вложений” и “возможностей”.

Пример специального маркера и ультрафиолетового фонаря.

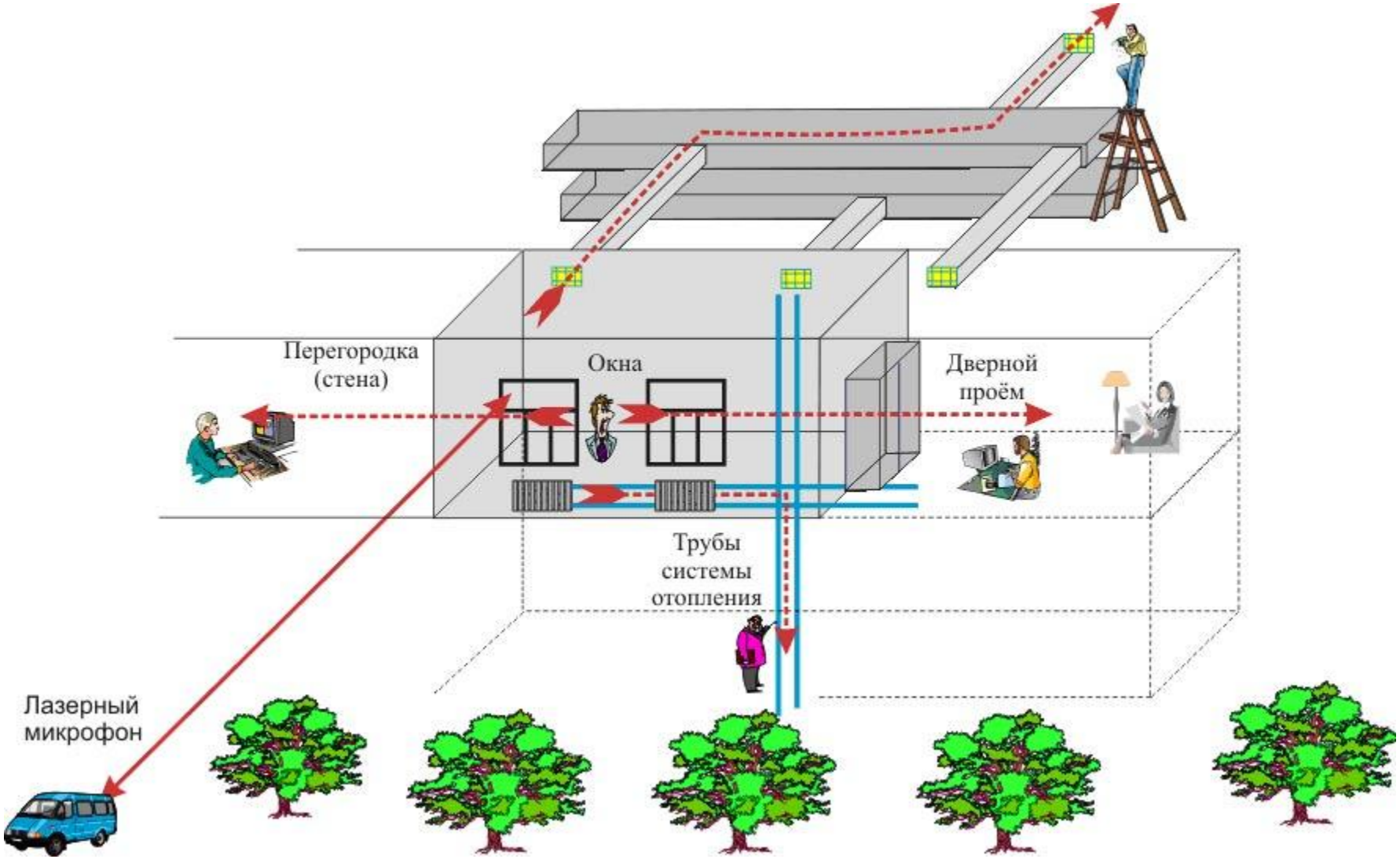
“Своя территория”.

“Беззаходовые” средства съёма информации не требуют проникновения злоумышленника в “нужное” помещение для их установки и практически не могут быть обнаружены в ходе осмотра данного помещения. Если говорить об угрозах, которые могут быть реализованы злоумышленниками в молдавском “коммерческо-частном секторе”, то вариант использования лазерной акустической системы разведки *(т.н. “лазерный микрофон”)* практически не реален (по целому ряду причин) – *моё личное мнение*. Использование т.н. “направленных микрофонов” в принципе возможно, но маловероятно, так как будет малоэффективно с точки зрения злоумышленника. Наиболее реальной угрозой является использование стетоскопов – в частности на тех объектах, где в одном здании размещаются несколько различных структур *(например, бизнес-центр с “поэтажной” арендой)* и где существует возможность доступа к “общим” элементам конструкции *(стены, полы, потолки)* или к техническим коммуникациям *(трубы, вентиляционные короба и т.д.)*, проходящим транзитом через помещения различных “хозяев”.

Нужно постоянно помнить о т.н. “**естественных каналах утечки информации**”: вентиляционных каналах и других “акустоводах”, не зашторенных окнах и т.д.

Вероятность данных угроз должна быть чётко определена и при необходимости для их блокирования должны быть приняты организационно-технические меры.

Примеры некоторых естественных каналов утечки акустической информации.



Пример идеального естественного “акустовода”, который имеется в большинстве зданий “новой постройки”.

Пример идеального естественного “акустовода”, который имеется в большинстве зданий “новой постройки”.

Вертикальные стойки, которые идут “сквозняком” через все этажи здания, являются идеальным “акустоводом” – учитывая, что они “полые” внутри.

Во-первых, эти стойки могут быть “проводником звука” – акустический сигнал может распространяться по ним через несколько этажей и перехватываться с помощью стетоскопа.

Во-вторых, эти стойки могут быть использованы злоумышленниками в качестве “футляра”, в котором будет находиться проводной микрофон. Микрофон может “спускаться” внутри стойки с верхних этажей или наоборот – может “проталкиваться” до нужного уровня с нижних этажей. Обнаружить микрофон внутри стойки практически невозможно – для этого нужно осмотреть весь “стояк”, что нереально в случае “поэтажной” аренды здания разными хозяевами.

Некоторые нюансы, которые могут возникнуть на “своей территории”.

Необходимо отметить, что если говорить о ЗИ на “своей территории”, то есть два случая, которые требуют особого подхода к этому вопросу:

Первый – это вариант, когда устройство аудио- или видеозаписи находится непосредственно у пришедшего к вам посетителя – т.е. вашу беседу “пишет” или “снимает” ваш собеседник (например, на диктофон или на видеорекордер). В этом случае вы или доверяете своему собеседнику *(решать вам)*, или необходим его физический досмотр – *что не всегда возможно выполнить как “технически”, так и “юридически”*.

Второй – это вариант, когда ваша компания размещается в арендуемом помещении – т.е. с одной стороны вы вроде бы и на “своей территории” *(организованы режимные мероприятия, посторонние бесконтрольно к вам не попадут и вроде бы всё хорошо)*, но с другой стороны реальный хозяин этого объекта *(арендодатель)* до вашего “вселения” имел все возможности по установке средств съёма информации *(в том числе с “глубоким камуфляжем”)*. В этом случае нужно вначале провести комплексную специальную проверку помещения с использованием всей необходимой поисковой техники – если есть такая возможность *(в том числе с привлечением “специалистов со стороны”)* или считать, что вы находитесь на “чужой территории” *(см. далее)*.

“Чужая территория” и её хозяин – “злоумышленник”.

В этом случае в помещении могут быть установлены самые различные средства съёма информации (аудио- и видеоконтроля).

Если объект *“был подготовлен”* для постоянного контроля за всеми “гостями”, то наиболее вероятна установка “проводных систем” – *как правило, закамуфлированных в предметы интерьера: датчики сигнализации, электроприборы, бытовая электронная техника и т.д*. – при этом для передачи информации могут использоваться как “штатные” проводные линии, проходящие через помещение, так и специально проложенные кабели. Теоретически возможен и “**глубокий камуфляж**” средств съёма информации – в этом случае данные устройства “прячутся” *(“замуровываются”)* в ограждающих конструкциях *(стенах, полах, потолках)*.

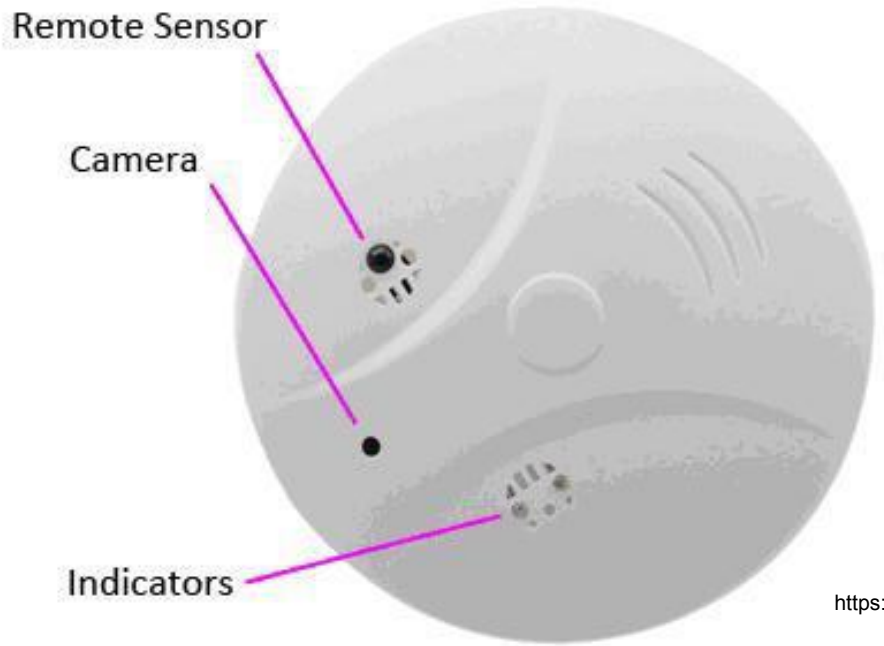
Если же хозяина объекта интересуют “разовые” посетители, то наиболее вероятна установка “в нужном месте и в нужное время” устройств аудио- и видеорегистрации *(диктофонов и видеорегистраторов)* – в том числе, закамуфлированных под бытовые предметы.

Кроме того, возможно использование средств аудио- и видеоконтроля с передачей информации по радиоканалу – *в большинстве случаев через Wi-Fi или через сеть сотовой связи* – в том числе, закамуфлированных.

Видеокамера и микрофон, установленные в датчике сигнализации.

Один из “типовых” вариантов камуфляжа устройств съёма информации.
Очень часто используется для организации стационарных систем скрытого видеонаблюдения.

Видеокамеры, установленные в датчике пожарной сигнализации и в “фальшивом” устройстве пожаротушения.



https://tscmamerica.com

Камера или микрофон могут быть спрятаны в различных типах датчиков системы охранно-пожарной сигнализации.

Кроме того, они могут быть установлены в “фальшивых” датчиках, которые вообще не подключены к системе ОПС.

Пример “глубокого камуфляжа” устройства съёма информации.

Устройство было “замуровано” в стене под обоями и прикрыто плинтусом.

Пример гостиничного номера.

“Экипировка” гостиничного номера:

Микрофоны были обнаружены случайно постояльцем, который на несколько дней остановился в данном номере. Причём, этот постоялец остановился в данной гостинице внезапно, так что маловероятно, чтобы гостиничный номер “заряжался” специально под него.

“Экипировка” гостиничного номера:

Судя по исполнению, микрофоны были установлены в номере работниками гостиницы для “постоянного контроля” за посетителями.

<u>Примечание</u>: нужно чётко понимать, что многие *“специфические”* гостиницы (например, большинство *“апартаментов”*, которые *“сдаются почасово”*) *“находятся под контролем”* – в связи *“со спецификой их посетителей”*.
Как говорится: *“Замочные скважины поинтересней нефтяных”*.

Скрытые видеокамеры, установленные в солярии.

Пример того, как скрытое видеонаблюдение осуществлялось за гражданами, находящимися на “чужой территории”, а в качестве “злоумышленника” выступал непосредственно “хозяин” этой “территории”.

Примечание: нужно чётко понимать, что практически все *“места досуга”* по определению *“находятся под контролем”* и после их *посещения* можно стать *“звездой экрана” (это ещё в лучшем случае)*.
Есть очень большая разница между баней (сауной) и *“баней” (“сауной”)*, массажем и *“массажем”*, не говоря уже о различного рода *“чистках чакр”*, *“активизации и обмене энергией любви”* и других *б******х вариантах*.

“Чужая территория” и её хозяин – “злоумышленник”.

На “чужой территории” аудио- и видеоконтроль могут осуществляться и без установки в помещениях каких-либо устройств съёма информации. Для этого “хозяином-злоумышленником” могут быть реализованы чисто “конструкторско-строительные решения”.

Причём эти “решения” могут быть как очень простыми – например, в стене “тупо” делается небольшое отверстие, через которое можно слушать и наблюдать, что происходит в соседнем помещении, так и достаточно сложными – например, установка в “нужном” помещении “прозрачных зеркал” *(т.н. “шпионское зеркало”)* или даже “прозрачных” стен *(потолков)*, выполненных по технологии “шпионского зеркала”.

Принцип работы “шпионского зеркала” – т.н. “зеркало Гезелла”.

Пример помещения, в котором установлено “шпионское зеркало”.

“Чужая территория”, на которой “злоумышленником” является не её хозяин, а “третье лицо”.

Как было сказано ранее, в этом случае может быть несколько вариантов.

Во-первых, “злоумышленником” может быть один из сотрудников, который там работает: например, работник гостиницы вполне может установить “что-то” в “нужном номере”.

Наиболее вероятна установка в “нужном помещении” диктофонов и видеорегистраторов (в том числе, закамуфлированных), которые будут периодически изыматься “злоумышленником”.

В ряде случаев возможна установка средств аудио- и видеоконтроля с передачей информации по радиоканалу – *в большинстве случаев через сеть сотовой связи или через Wi-Fi* – в том числе, закамуфлированных.

Многое зависит от того, на кого “работает” этот сотрудник: на самого себя (по принципу: *“нехай будет – может когда пригодится”*) или у него есть “заказчик”, которого интересуют конкретные моменты. Также многое зависит от рода деятельности злоумышленника: у охранника “на вахте”, горничной и администратора гостиницы разные возможности.

Скрытые видеокамеры, установленные в туалете гостиницы.

Писающие мальчики по-когалымски: в туалете отеля велась видеосъемка

28.08.2012 | 14:59

Tweet 13 Сохранить В 9

Я рекомендую 18 пользователей рекомендуют это. Sign Up, чтобы посмотреть рекомендации друзей

В мужском туалете одной из 4-звездочных гостиниц города Когалыма (ХМАО) велась скрытая видеосъемка. Это обнаружилось, когда видео выложили в Интернет. По всей видимости, это дело рук недобросовестных сотрудников гостиницы. Сопровождались эти кадры ехидными и циничными комментариями, сообщает Life News.

На записи видно, как клиенты отеля, не подозревая, что за ними следят, занимаются своими делами: выходят и заходят в кабинки, переодеваются, моют руки и прихорашиваются перед зеркалом.

Полиция Когалыма уже начала проверку по факту незаконных съемок. Если шутники будут найдены, им грозит крупный штраф или арест, поскольку это деяние трактуется статьей 137 УК РФ "Нарушение неприкосновенности частной жизни".

Пример того, как скрытое видеонаблюдение осуществлялось за гражданами, находящимися на “чужой территории”, а в качестве “злоумышленника” выступало “третье лицо”, имеющее постоянный доступ на эту “территорию” – в данном случае это был один из сотрудников гостиницы.

*Причём этот долб**б снимал скорее всего для того, чтобы просто “поприкалываться”.*

“Чужая территория”, на которой “злоумышленником” является не её хозяин, а “третье лицо”.

Во-вторых, “злоумышленником” может быть абсолютно посторонний человек, который с определённой периодичностью посещает эту “территорию”.

Если “злоумышленник” посещает объект достаточно часто: например, он постоянно бронирует себе в гостинице один и тот же номер или является постоянным посетителем *“массажного салона”*, то наиболее вероятна установка им в “нужном помещении” диктофонов и видеорегистраторов *(в том числе, закамуфлированных)*, которые будут периодически им изыматься.

Если же “злоумышленник” посетил объект “разово”: *например, заехал на несколько дней в гостиницу*, то наиболее вероятна установка им средств аудио- и видеоконтроля с передачей информации по радиоканалу – *как правило, через сеть сотовой связи* – в том числе, закамуфлированных.

Естественно, что у такой категории “злоумышленников” возможностей гораздо меньше, чем у постоянных работников данного объекта.

Ещё раз об угрозах на “чужой территории”.

Нужно чётко понимать и постоянно помнить, что “**чужая территория**” – **это по определению** “**зона повышенной опасности**” **в плане возможного съёма информации**.

Причём речь идёт не только о “конкретном человеке”, за которым могут “наблюдать”. Можно совершенно случайно “попасть в историю”, находясь в каком-либо “общественном месте”: гостиница, ресторан, база отдыха и т.д. *(не говоря уже о различного рода “банях” и “массажных кабинетах”)*, в котором ведётся скрытый аудио- и видеоконтроль всех посетителей.

Что же касается возможности проведения проверки, то на “чужой территории” она в большинстве случаев ограничена, а **иногда в принципе невозможна**: например, свой гостиничный номер осмотреть можно *(более-менее)*, в ресторане можно осмотреть столик *(плюс-минус)*, а вот проведение осмотра *“бани”* или *“массажного кабинета”* практически нереально без согласия хозяина.

Поэтому при нахождении на “чужой территории” нужно отталкиваться от того, что за вами возможен постоянный контроль, и вести себя соответственно: **не “болтать лишнего”** (помнить “*Что говорю? Кому говорю? Когда и где говорю?*”) и **не “делать лишнего”** – если только вы не *“поклонник свободной любви без всяких обязательств” (см. далее)*.

Вариант “*универсальной защиты от всех проблем*”... или “*почти от всех*”.

Мюллер взял яблоко, лежавшее на столике охраны, и сказал:

– Неудобно идти без подарка. Даже если мы оба поклонники свободной любви, без всяких обязательств, и тогда к бывшим дружкам надо идти с подарком.

Штирлиц заставил себя рассмеяться: он понял, отчего так сказал Мюллер. Однажды его люди пытались завербовать южноамериканского дипломата; они показали ему несколько фотографий – дипломат был снят в постели с белокурой девицей, которую подсунули ему люди Мюллера. “Либо, – сказали ему, – мы перешлём эти фото вашей жене, либо помогите нам”. Дипломат долго рассматривал фотографии, а потом спросил: “А нельзя ли мне с ней полежать ещё раз? Мы с женой обожаем порнографию”. Это было вскоре после приказа Гиммлера – обращать особое внимание на семейную жизнь немецких разведчиков. Штирлиц тогда ворчал: “Надо исповедовать свободную любовь без всяких обязательств, тогда человека невозможно поймать на глупостях”.

Когда ему рассказали об этом случае, Штирлиц только присвистнул: “Найдите мне такую жену, которая любит порнографию, я сразу отдам ей руку и сердце. Только, по-моему, перуанец вас переиграл: он испугался своей жены до смерти, но не подал вида и сработал, как актёр, а вы ему поверили.

Ты бы испугался своей жены? Конечно! А меня не возьмёшь – я боюсь только самого себя, ибо у меня нет ни перед кем никаких обязательств. Единственное, что плохо, – некому будет приносить в тюрьму передачи”.

Юлиан Семёнов, “Семнадцать мгновений весны”.

Примечание: на самом деле у Максима Максимовича Исаева (Владимирова) – *он же Штирлиц* – отношения с женой были совсем другими. Наиболее полно им соответствует фраза, которую оставил своей жене в посмертном письме один известный писатель XIX века:

“***Я любил только тебя и не изменял тебе ни разу, даже мысленно***”.

Некоторые “общие” моменты, касающиеся проведения визуального осмотра помещения с целью поиска устройств съёма информации.

Когда речь идёт о поиске устройств съёма информации, то нужно чётко понимать и постоянно помнить, что злоумышленник может использовать не только какое-либо *“явное” устройство съёма информации*, которое будет установлено в помещении и которое “*можно увидеть глазами и пощупать руками*”.

В ряде случаев съём *(утечка)* информации может осуществляться за счёт т.н. “**естественных каналов утечки информации**” *(разной физической природы)*, различных “**штатных**” **функций** телекоммуникационного оборудования или различного рода “**программных закладок**” – образно говоря, эти угрозы имеют совсем другой “внешний вид” и их нельзя *“увидеть и пощупать”* при проведении визуального осмотра помещения *(в классическом понимании)*.

Для выявления данных угроз требуется **особая подготовка сотрудников**, наличие специального оборудования – *для выявления “естественных каналов утечки”* и специального программного обеспечения *(по аналогии с “антивирусами”)* – *для выявления “программных закладок” (в том числе т.н. Spy-Phones)*.

Моё личное мнение: **реальным поиском** указанных выше угроз **может заниматься только специально подготовленный человек**, имеющий базовое техническое образование и хорошо понимающий “физику” и “логику” их возникновения – *это возможно только в серьёзных компаниях где “всё по взрослому”*.

Некоторые “общие” моменты, касающиеся проведения визуального осмотра помещения с целью поиска устройств съёма информации.

В большинстве реальных случаев, когда вопросами защиты информации в компании занимается не специально подготовленный человек, а они возложены “по совместительству” на сотрудника личной охраны *(возможно, прошедшего какую-то краткосрочную подготовку в этой области)*, данному сотруднику нет смысла вообще “заморачиваться” на поиск каких-либо “сложных” вариантов угроз – он должен сосредоточиться именно на тщательном визуальном осмотре помещения.

При этом, по большому счёту, такого “поисковика” не должно интересовать как именно “работает” возможно внедрённое устройство съёма информации – *в режиме “накопителя”, в режиме радиопередатчика, передаёт информацию по проводной линии и т.д.* – в этом случае основной “критерий оценки” обнаруженных предметов должен быть: “**Что это такое и как оно сюда попало**?”.

Естественно, что в ходе визуального осмотра помещения такой “поисковик” должен обращать внимание и на различного рода “явные” естественные каналы утечки информации: *постоянно открытое окно, явно плохая звукоизоляция – когда в соседнем помещении “всё слышно невооружённым ухом” и т.п.*

В то же время, данный сотрудник должен иметь представление об указанных выше “нестандартных” угрозах и при необходимости предложить руководству вызвать подготовленного “специалиста со стороны” для их выявления и оценки.

Немного о “внешнем виде” устройств съёма информации.

Когда речь идёт о визуальном осмотре помещения с целью обнаружения возможно установленных средств съёма информации, то “поисковик” должен чётко себе представлять “***что он ищет и как оно может выглядеть***”.

“Внешний вид” устройств съёма информации, используемых в “коммерческо-частном секторе”, может быть различным, но можно выделить две основные группы таких устройств: изделия в “обычном” исполнении и изделия в “камуфлированном” исполнении.

С устройствами съёма информации, имеющими “обычное” исполнение, всё *“относительно просто”* – внешне они представляют собой “предмет непонятного назначения” в виде “отдельного модуля” или “закрытой коробочки”, который можно “увидеть и пощупать” в ходе проведения осмотра и понять, что это – “закладка”.

В то же время с устройствами съёма информации, которые имеют “камуфлированное” исполнение, всё намного сложнее.

В ряде случаев *(например, в случае “**глубокого камуфляжа**”)* такие устройства в принципе нельзя “увидеть”*(т.е. идентифицировать как “закладку”)*, даже держа их прямо в руках *(моё личное мнение) – для их “идентификации” потребуется использование специального поискового оборудования*.

С точки зрения “внешнего вида” можно выделить несколько основных вариантов исполнения устройств съёма информации, которые могут быть использованы злоумышленниками в “коммерческо-частном секторе”:

- Устройства, выполненные в виде нескольких соединённых между собой отдельных “открытых модулей”: обычно это “основной” электронный модуль и источник электропитания *(батарея или аккумулятор)*.
- Устройства, выполненные в виде одного “закрытого модуля” – образно говоря, это “коробочка” (единый корпус), в которой размещены все элементы закладного устройства, включая источник электропитания.
- Устройства “заводского изготовления”, камуфлированные в предметы интерьера и имеющие автономное электропитание *(батареи или аккумуляторы)*.
- Устройства в виде “отдельных модулей”, установленные в различные электроприборы и электронную технику (в том числе, установленные “самостоятельно” злоумышленником).
- Устройства “заводского изготовления”, камуфлированные в различные электроприборы и электронную технику.
- Устройства, устанавливаемые в телекоммуникационное оборудование или подключаемые к телекоммуникационным линиям.
- Различные проводные системы, состоящие из “основного” электронного модуля – *микрофона или камеры*, соединённого с проводной линией *(кабелем)*.
- Устройства “бытового назначения”, которые в ряде случаев могут быть использованы злоумышленниками для съёма информации.

Приведённая выше “классификация” является достаточно условной и охватывает только те типы устройств съёма информации, которые могут быть внедрены в помещение и которые можно “*увидеть и пощупать*” при проведении визуального осмотра.

Устройства съёма информации, выполненных в виде отдельных “открытых модулей”.

Устройства данного типа выполнены в виде нескольких соединённых между собой отдельных “модулей” – как правило, это “основной” электронный модуль *(радиомикрофон или камера)* и источник электропитания *(батарея или аккумулятор)*.
Модули могут представлять собой как “открытую” электронную плату, так и могут находиться в “термоусадке” или быть “залитыми” компаундом.

Такой вариант наиболее характерен для “самодельных” закладных устройств, но некоторые профессиональные “закладки” тоже могут иметь такой внешний вид.

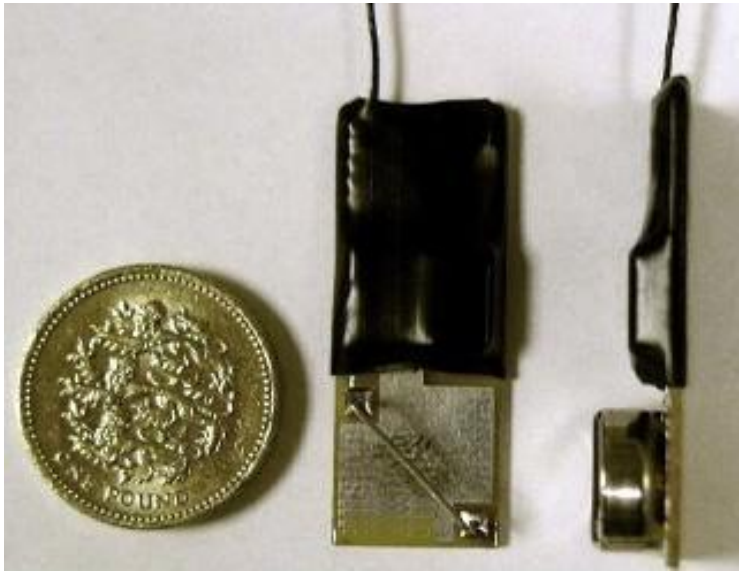
Важный момент: в настоящее время всё большее распространение получают “модульные” Wi-Fi видеопередатчики – в том числе с накоплением информации, которые позиционируются производителями как “*охранные системы*”.

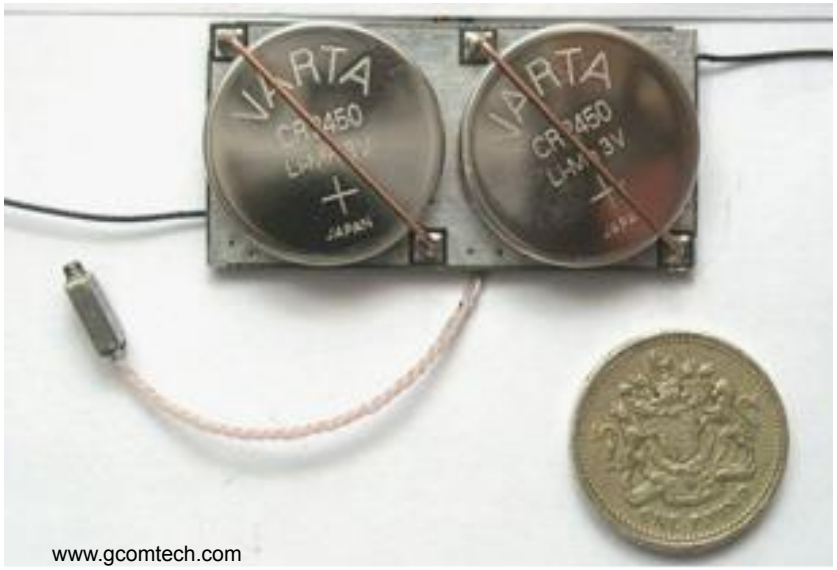
Данные устройства достаточно легко обнаружить при проведении тщательного визуального осмотра помещения – так как внешне они представляют “явно подозрительный предмет непонятного назначения”.

Самодельные радиомикрофоны, выполненные в виде отдельных “открытых модулей”.

www.xn--80ahmllff5e0c.xn--p1ai/

Профессиональные радиомикрофоны, выполненные в виде отдельных “открытых модулей”.





Как правило, профессиональные “модульные закладки” предназначены для последующего камуфлирования, но иногда злоумышленники могут использовать их и в “чистом виде”, особо не заморачиваясь на камуфляж.

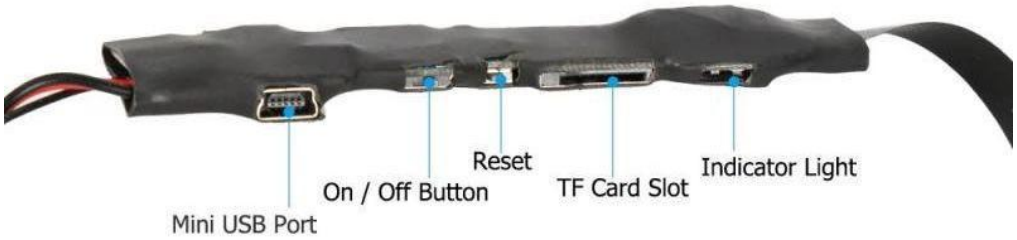
“Модульные” Wi-Fi видеопередатчики.

Данные устройства в настоящее время широко распространены – *они позиционируются производителями как “охранные системы”* и практически свободно продаются через различные “интернет-магазины”.

“Модульные” Wi-Fi видеопередатчики бывают различных типов: некоторые работают только в режиме реального времени и начинают передавать сигнал сразу после включения, другие имеют в своём составе элемент памяти и могут предварительно накапливать информацию, а потом передавать её по Wi-Fi на приёмный пункт. Некоторые модели предназначены только для передачи видео, а в других имеется и встроенный микрофон.

Для данных изделий возможны различные варианты электропитания: от аккумулятора (“штатный” вариант) или от сети 220 В через миниатюрный преобразователь.

Пример типового “модульного” Wi-Fi видеопередатчика.



Пример “модульного” Wi-Fi видеопередатчика с накоплением информации.

Профессиональный “модульный” Wi-Fi передатчик с накоплением информации. Возможны различные варианты работы изделия: передача видео по Wi-Fi в реальном масштабе времени или запись видео на карту памяти с последующей его передачей по Wi-Fi.
Управление осуществляется с помощью беспроводного пульта ДУ *(радиоканал)*.
Минимальное время работы от штатного аккумулятора – 180 минут.

Устройства съёма информации, выполненных в виде одного “закрытого модуля”.

Данные изделия выполнены в виде “единой закрытой коробочки”, в которой находятся все элементы закладного устройства (в том числе и источник электропитания).

По сравнению с изделиями, состоящими из нескольких “отдельных модулей”, данные устройства намного компактнее и удобнее – в них всё находится внутри надёжного корпуса, ничего *“не болтается”* и *“не висит”*.

Такой вариант наиболее характерен для большинства устройств съёма информации, которые используются в “коммерческо-частном секторе”: диктофоны, автономные видеорегистраторы, GSM-передатчики и т.д.

Данные устройства достаточно легко обнаружить при проведении тщательного визуального осмотра помещения – так как внешне они представляют собой “подозрительный предмет непонятного назначения”.

Примеры диктофонов *(диктофоны серии EDIC-mini)*.

Примеры видеорегистраторов, выполненных “единым модулем”.

www.pimall.com

www.telesys.ru

Примеры Wi-Fi–передатчиков и GSM–передатчиков, выполненных в виде единого “закрытого модуля”.

www.acustek.com

www.spytome.net

Устройства съёма информации “заводского изготовления”, камуфлированные в предметы интерьера и имеющие автономное питание.

Данные изделия могут быть выполнены в виде самых различных предметов, которые используются в повседневной жизни – при этом практически полностью сохраняются все “штатные” функции данных предметов: калькулятора, настольных часов, пульта ДУ, авторучки, маркера и т.д. В таком исполнении могут быть выполнены различные типы устройств съёма информации – как “накопители” *(диктофоны и видеорегистраторы)*, так и “радиопередатчики” *(аудио- и видео)*.

Такой вариант достаточно распространён для устройств съёма информации, которые используются в “коммерческо-частном секторе”: в частности, камуфлированные диктофоны и автономные видеорегистраторы практически свободно продаются во многих “интернет-магазинах”.

*Обнаружение данных устройств – имеется ввиду идентификация их как устройств съёма информации – в ходе проведения визуального осмотра помещения **может быть весьма проблематичным**, так как внешне они представляют собой какой-нибудь “самый обычный предмет”.*

Устройства съёма информации “заводского изготовления”, камуфлированные в предметы интерьера и имеющие автономное питание.

В ряде случаев наличие “закладки” может быть обнаружено в ходе разборки предмета, внутри которого она установлена: *в первую очередь это касается устройств, в которых предусмотрена “самостоятельная” замена элементов питания, “зарядка” встроенного аккумулятора или установка SIM-карты (для GSM-передатчиков).*

В то же время, целый ряд камуфлированных устройств съёма информации в принципе не может быть идентифицирован в ходе визуального осмотра – даже если он проводится тщательно и добросовестно *(моё личное мнение)*.

В частности, речь идёт о камуфлированных устройствах съёма информации, в которых не предусмотрена “самостоятельная” замена *(“зарядка”)* элементов питания, а сам “предмет” является “неразборным” – *например, вариант “классического” радиомикрофона, “вшитого” в кожаную папку или в толстую книжную обложку*.

Обнаружить такое изделие можно только с помощью поисковых технических средств или путём “явного повреждения” корпуса данного предмета *(а не его “разборки”)*.

Поэтому при осмотре предметов необходимо обращать внимание не только на различные внешние “технические” детали: наличие небольших отверстий (“наколов”) в корпусе, непонятных конструктивных элементов, слотов под SIM-карту или под карту памяти, мини-разъёмов и т.д., но и уточнять “общие” вопросы:

откуда этот предмет вообще здесь взялся и что он тут делает?

Устройства съёма информации “заводского изготовления”, камуфлированные в предметы интерьера и имеющие автономное питание.

Нужно отметить один момент, касающийся “долговременности” возможной работы камуфлированных устройств съёма информации с автономным питанием, который косвенно связан с их обнаружением в ходе визуального осмотра помещения.

С устройствами типа “накопителя” *(диктофоны и видеорегистраторы)* всё ясно – злоумышленник в любом случае должен повторно попасть в “нужное” помещение, чтобы изъять “накопленные” записи.

Соответственно, если у него есть возможность периодического свободного доступа в ваше помещение, то он может осуществлять и замену элементов питания в “накопителе”.

Аналогичная ситуация и с радиопередающими устройствами – если злоумышленник имеет свободный доступ на объект, то он может по мере необходимости менять элементы питания в “занесённой” к вам “закладке”.

Такая ситуация характерна для случаев, когда вы находитесь на “чужой территории”, а так же когда вы на “своей территории”, но у вас там “полный бардак” и “проходной двор” или в вашем ближайшем окружении есть “засланный казачёк”.

Как было сказано ранее, если речь идёт о “своей территории”, то в этом случае одних “поисковых” мероприятий будет мало – в первую очередь, нужно правильно организовать режим на вашем объекте.

Ну а на “чужой территории” нужно помнить о возможном “контроле за вами” и быть “бдительным” (в хорошем смысле этого слова) – об этом тоже было сказано ранее.

Устройства съёма информации “заводского изготовления”, камуфлированные в предметы интерьера и имеющие автономное питание.

Совсем другое дело, когда камуфлированная “радиозакладка” с автономным питанием была каким-то образом внедрена к вам на объект “разово” и у злоумышленника нет возможности попасть туда повторно для замены элементов питания – *считаем, что “режим на уровне”, все сотрудники “проверены” и т.д*.

Если речь идёт о **“простом” варианте**, то “закладка” работает некоторое время, пока у неё не закончится питание и она *“не умрёт”*. Такое устройство может работать достаточно длительное, но “ограниченное” время – всё зависит от мощности, наличия ДУ, ёмкости источника питания и ряда других факторов.

Но возможен и **“сложный” вариант** *(который принципиально отличается)* – речь идёт о радиомикрофонах, камуфлированных в предметы интерьера, имеющие свой “штатный” элемент питания, который необходимо периодически менять или подзаряжать для нормальной работы “основного” *(“легального”)* изделия: калькулятор, пульт ДУ, электронные часы, мобильный телефон, электронная игрушка и др. Получается, что в этом случае периодическую замену *(подзарядку)* элементов питания осуществляет не “злоумышленник”, а сам хозяин *(которого “слушают”)* – даже не подозревая, что он “заряжает” не только “основное изделие”, но и “встроенную закладку”.

Поэтому на предметы интерьера, имеющие “штатную” батарею или аккумулятор, нужно обратить особое внимание и они должны быть проверены особенно тщательно.

Примеры камуфлированных диктофонов.

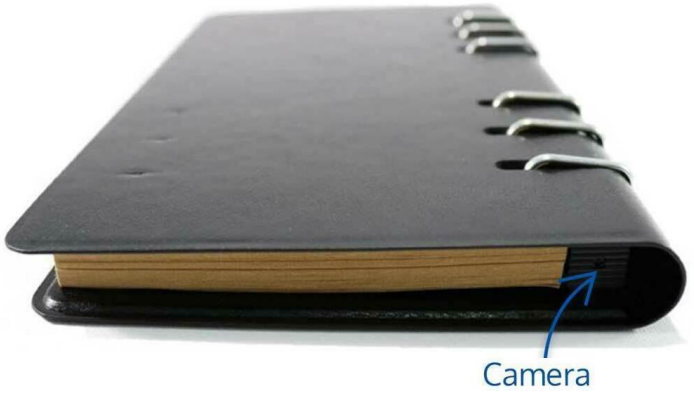
www.spyshop-online.com

Диктофон, закамуфлированный в брелок и в автомобильный ключ.

Примеры камуфлированных диктофонов.

Диктофон в виде банковской карточки может быть установлен практически в “любую щель”.
Технические возможности таких изделий (система VOX, таймер, аккумулятор и т.д.) позволяют вести аудиозапись в течении длительного времени и с высоким качеством.

Примеры камуфлированных видеорегистраторов.



Некоторые бытовые предметы, в которых могут быть закамуфлированы ЗУ с передачей информации по радиоканалу.

Пример камуфляжа ЗУ с передачей информации по радиоканалу.

Time of continuous operation	Dimensions(mm)
12 days	140 x 100 x 7
12 days	200 x 150 x 4
24 days	200 x 210 x 4
36 days	290 x 210 x 4

Пример GSM–передатчика “заводского изготовления”, камуфлированного в “штатном” аккумуляторе мобильного телефона.

www.radioscanner.ru/forum/topic41066-1.html

Данное изделие имеет очень высокий уровень камуфляжа и представляет собой GSM-передатчик, установленный в “штатный” работающий аккумулятор мобильного телефона. Фактически от данного аккумулятора одновременно работают два “независимых” радиопередающих устройства: “основной” мобильный телефон *(через свою “штатную” SIM-карту)* и “GSM-закладка” *(через свою “секретную” SIM-карту)*. Зарядку аккумулятора осуществляет сам владелец мобильного телефона, который ничего не подозревает.

Устройства в виде “отдельных модулей”,
установленные в различные электроприборы и электронную технику
(в том числе, установленные “самостоятельно” злоумышленником).

Данные изделия выполнены на базе типовых “отдельных модулей”, которые для обеспечения их непрерывного электропитания устанавливаются в штатные электроприборы и электронную технику: электроудлинители, электророзетки, настольные лампы, датчики ОПС, бытовую технику и т.д.
В большинстве случаев такие “закладки” подключаются через миниатюрный адаптер *(“блок питания”)* к цепям 220 В, но если в электронной технике есть “штатные” низковольтные цепи – *например, в датчиках ОПС или в USB-портах*, то они могут быть подключены непосредственно к ним “напрямую”.

Такой вариант характерен для многих устройств съёма информации, которые используются в “коммерческо-частном секторе” и предназначены для долговременной “работы”: в первую очередь это “радиопередатчики” *(аудио- и видео)* – в том числе с передачей по GSM и Wi-Fi.

Данные устройства достаточно легко обнаружить при проведении тщательного визуального осмотра путём вскрытия электронной техники и электроприборов – так как внешне они представляют собой “подозрительный предмет непонятного назначения”, размещённый внутри.

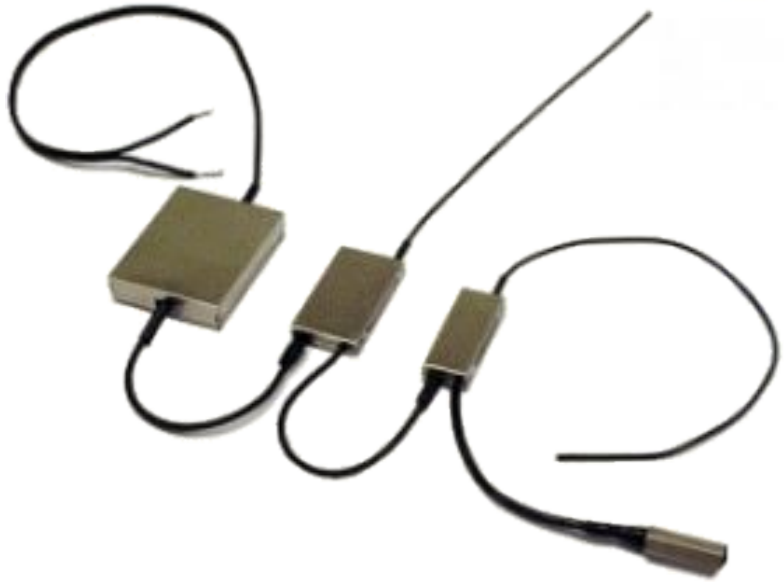
Некоторые бытовые электроприборы, в которые могут быть установлены закладные устройства в виде “отдельных модулей”.

www.pixcucamera.com

Примеры “модульных” радиомикрофонов, которые могут быть установлены внутри бытовой электроники и “запитаны” от неё.

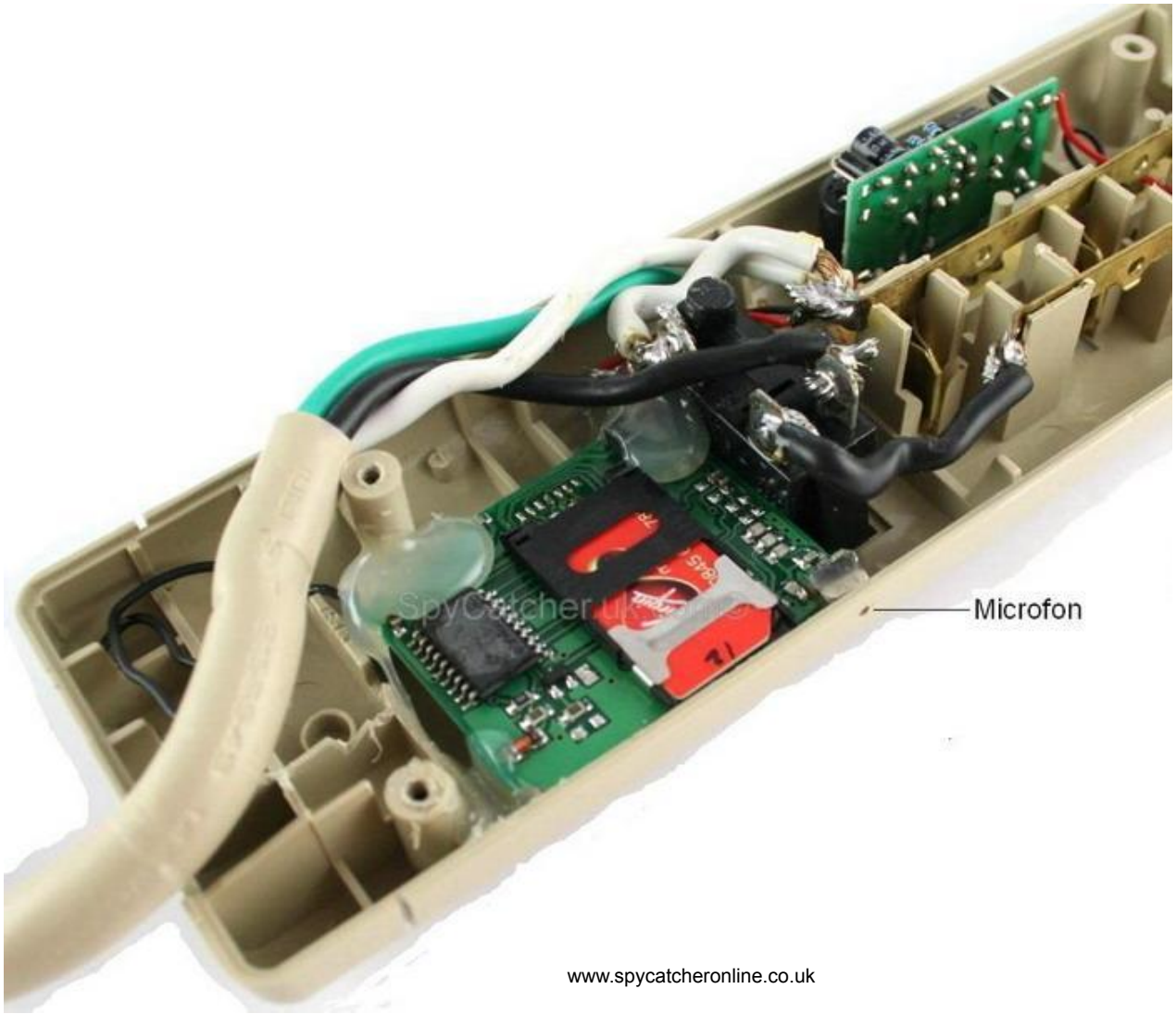
Установленные внутри электроники “модульные” радиомикрофоны могут быть “запитаны” как напрямую от “низковольтных” цепей – *если есть такая возможность*, так и через миниатюрный адаптер от цепей с напряжением 220 В.

www.spy-shop.com



www.endoacustica.com

Пример “модульного” GSM-передатчика, установленного в электроудлинитель.



www.spycatcheronline.co.uk

Пример “модульного” GSM–передатчика, закамуфлированного в “мышь”.

Пример “модульного” Wi-Fi видеопередатчика, который может быть установлен внутри бытовой электроники и “запитан” от неё.

“Модульный” Wi-Fi передатчик, который может быть установлен внутри бытовой электроники и “запитан” как напрямую от “низковольтных” цепей – *если есть такая возможность*, так и через миниатюрный адаптер от цепей 220 В.

Устройства “заводского изготовления”, камуфлированные в различные электроприборы и электронную технику.

Устройства съёма информации “заводского изготовления” могут быть выполнены в виде самых различных электроприборов и электронной техники – при этом полностью сохраняются работоспособность и все “штатные” функции бытовой электронной техники, внутри которой находится “закладка”.

В таком исполнении могут быть выполнены различные типы устройств съёма информации – как “накопители” *(диктофоны и видеорегистраторы)*, так и “радиопередатчики” *(аудио- и видео)*.

Некоторые из таких устройств позиционируются производителями как “*охранные системы*” и практически свободно продаются во многих “интернет-магазинах”.

Обнаружение данных устройств – имеется ввиду идентификация их как устройств съёма информации – в ходе проведения ***визуального осмотра может быть весьма проблематичным****, а* ***в ряде случаев вообще невозможным*** *(моё личное мнение).*

Устройства “заводского изготовления”, камуфлированные в различные электроприборы и электронную технику – некоторые особенности.

В отличие от рассмотренных ранее устройств съёма информации, представляющих собой “отдельные модули”, установленные *(в том числе “самостоятельно”)* в электроприборы и электронную технику, данные изделия имеют принципиальные особенности, усложняющие их обнаружение в ходе визуального осмотра даже “вскрытой” электроники.

Устройства “заводского изготовления”, камуфлированные в электронную технику, изначально разрабатываются *(проектируются)* и изготавливаются как составная часть “основного” *(“штатного”)* электронного прибора – соответственно, внешне они не представляют собой “*отдельный модуль непонятного назначения*”, который “*подпаян к проводам питания где-то внутри электроприбора*”. Наоборот, **монтаж такой “закладки” выполнен практически “заподлицо” с остальными элементами соответствующей модели электронной техники и по внешнему виду не отличается от “общей картины”**.

Для “коммерческо-частного сектора” наиболее характерны варианты устройств съёма информации “заводского изготовления”, камуфлированных в небольшие электроприборы и малогабаритную электронную технику: электролампочка, блок питания, зарядное устройство, Wi-Fi рутер, музыкальный центр и т.п.

Устройства “заводского изготовления”, камуфлированные в различные электроприборы и электронную технику – некоторые особенности.

Основными демаскирующими элементами будут микрофон и видеокамера.

В первую очередь **видеокамера** – она в любом случае должна “иметь выход наружу”, чтобы “видеть” объект съёмки, поэтому в корпусе “основного” *(“штатного”)* электронного прибора обязательно должно быть отверстие под её объектив. Кроме того, камера всегда будет расположена возле отверстия в стенке корпуса “штатного” электроприбора – это в случае его “разборки” и осмотра изнутри.

В случае “**чисто акустической закладки**” ситуация с её обнаружением будет намного сложнее, чем с “видеозакладкой”: **во-первых**, для работы микрофона совсем не обязательно наличие специального отверстия в корпусе “основного” электронного прибора – звук может проникать просто через стенки корпуса; **во-вторых**, в изделиях “заводского изготовления” микрофон может быть размещён так, что его практически не будет видно даже при осмотре вскрытого “штатного” электронного прибора.

Ещё одним демаскирующим признаком, характерным для некоторых типов устройств съёма информации “заводского изготовления”, камуфлированных в электроприборы и электронную технику, будет наличие слотов под карту памяти – *для “накопителей”* или под SIM-карту – *для GSM-передатчиков*.
Поэтому при осмотре **нужно обращать внимание** на возможные “щели” для карточек.

Устройства “заводского изготовления”, камуфлированные в различные электроприборы и электронную технику – некоторые особенности.

Возможен и самый плохой *(с точки зрения обнаружения)* вариант:
акустическая “закладка” заводского изготовления – *в виде Wi-Fi передатчика с ДУ или “классического” радиомикрофона (тоже с ДУ)* – камуфлированная в электронную технику, которая имеет неразборный (“литой”) корпус – например, блок питания для ноутбука.

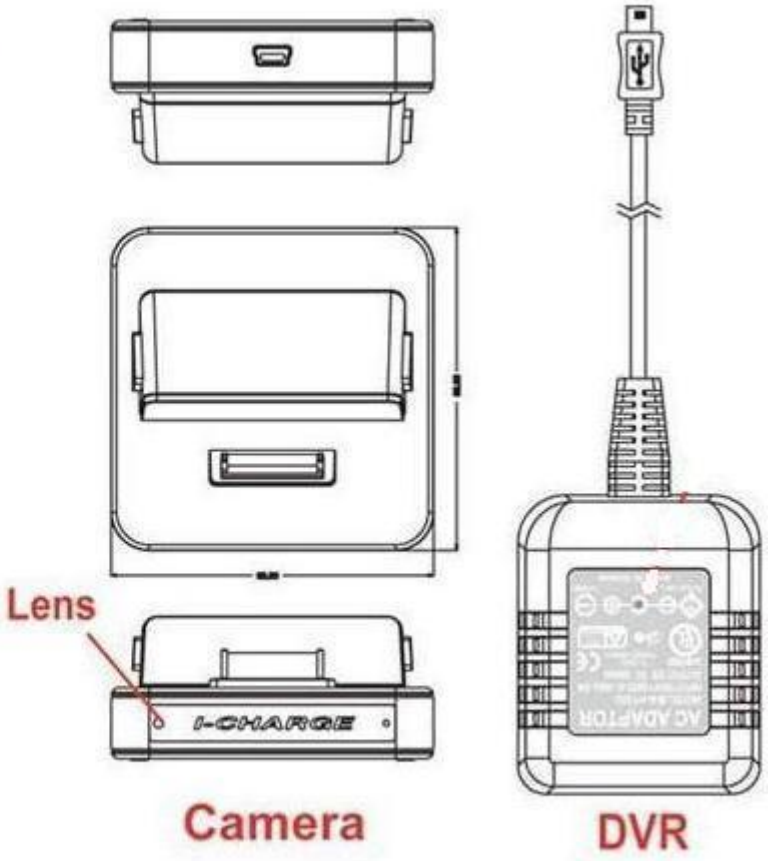
Визуальный осмотр в этом случае ничего не даст: нет никаких “внешних признаков” возможной установки “закладки” – так как отверстия (“накола”) для микрофона в корпусе может вообще не быть, а разобрать корпус нельзя – он “литой”.

Более того, многие поисковые технические средства в этом случае тоже бесполезны:

- Нелинейным локатором там проверять нечего – это “штатная” электроника.
- Проверка с помощью средств рентгеноскопии может ничего не дать – *если только исследование проводится не в специализированной лаборатории* – так как при рентгеноскопии “штатной” электроники есть **очень много** “нюансов”.
- Учитывая, что это изделие с дистанционным управлением (ДУ), обнаружить факт радиоизлучения можно будет только в тот момент, когда злоумышленник включит его на “передачу” – соответственно, для обнаружения такой “радиозакладки” должен быть организован **круглосуточный радиомониторинг** с использованием **реально работающих**, а не *“имитирующих бурную деятельность”* комплексов радиоконтроля.

Понятно, что если такая “закладка” попадёт на “среднестатистический” с точки зрения защиты информации объект, то она сможет работать там неограниченное время: электропитание у неё будет постоянно, а вероятность её обнаружения в ходе “периодических” проверок очень мала.

Пример профессионального видеорекордера, камуфлированного в зарядном устройстве.



www.pimall.com

Пример профессиональных видеорекордеров, камуфлированных в Wi-Fi рутер, USB-станцию и в блок питания.

www.onlinespyshop.co.uk

Данные изделия могут работать как в режиме “чистого накопителя” – записывая аудио- и видеоинформацию в память, так и осуществлять “промежуточное” накопление информации с последующей её передачей по радиоканалу *(обычно через Wi-Fi)*.

Пример “GSM-передатчика”, камуфлированного в зарядном устройстве.

Данное изделие является полноценным зарядным устройством, но при этом может перехватывать акустическую информацию и передавать её по сети GSM на “контрольный пункт”, который может находиться где угодно.
При этом специального отверстия (“накола”) в корпусе может и не быть – микрофон разборчиво принимает речь даже через стенки корпуса.

“Умная лампа” со встроенной видеокамерой и микрофоном.

Так называемые “умные лампы”, которыми можно управлять дистанционно по Wi-Fi, получают всё большую популярность. Лампа выполняет свою “штатную функцию” – *т.е. свет*, а кроме того имеет в своём составе встроенные камеру и микрофон. Такие “закладки” производятся на основе т.н. “экономичных” ламп с подсветкой на основе LED, в корпусах которых можно разместить микрофон, камеру и Wi-Fi передатчик – *в отличие от классических ламп накаливания, в “колбе” которых ничего установить нельзя, так как там вакуум и температура в несколько сотен градусов*.

Обычно данные изделия заявлены производителями как “системы охранного наблюдения”.

Устройства, устанавливаемые в телекоммуникационное оборудование или подключаемые к телекоммуникационным линиям.

По своему назначению устройства съёма информации, устанавливаемые в телекоммуникационное оборудование или подключаемые к телекоммуникационным линиям, могут быть **двух типов**:

- во-первых, это устройства, предназначенные для перехвата информации, циркулирующей в телекоммуникационных сетях *(телефонных переговоров)*.

- во-вторых, это устройства, которые предназначены для перехвата речевой и видовой информации из помещения, а от телекоммуникационного оборудования они только “запитаны”.

Внешний вид данных устройств может быть самый различный: они могут быть выполнены как в виде *“отдельных модулей непонятного назначения”*, устанавливаемых в абонентское оборудование или подключаемых к линии, так и в виде *“штатных”* элементов телефонного оборудования *(микрофонный капсюль, телефонная розетка, конденсатор и т.д.)*, которые внешне не имеют каких-либо “подозрительных признаков” и при визуальном осмотре очень часто не могут быть идентифицированы как “закладка”.

Устройства, устанавливаемые в телекоммуникационное оборудование или подключаемые к телекоммуникационным линиям.

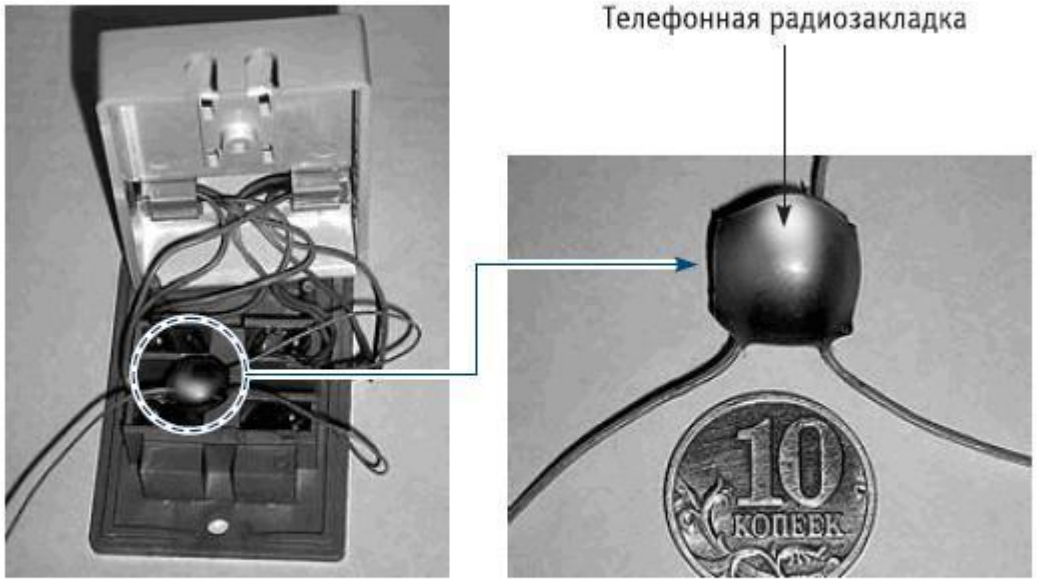
Обнаружение данных устройств – имеется ввиду идентификация их как устройств съёма информации – в ходе проведения ***визуального осмотра может быть весьма проблематичным****, а* ***в ряде случаев вообще невозможным*** *(моё личное мнение).*

Когда речь идёт о визуальном осмотре телекоммуникационного оборудования на предмет обнаружения возможно установленных устройств съёма информации, то нужно чётко понимать, что здесь возможны две принципиально разные ситуации:

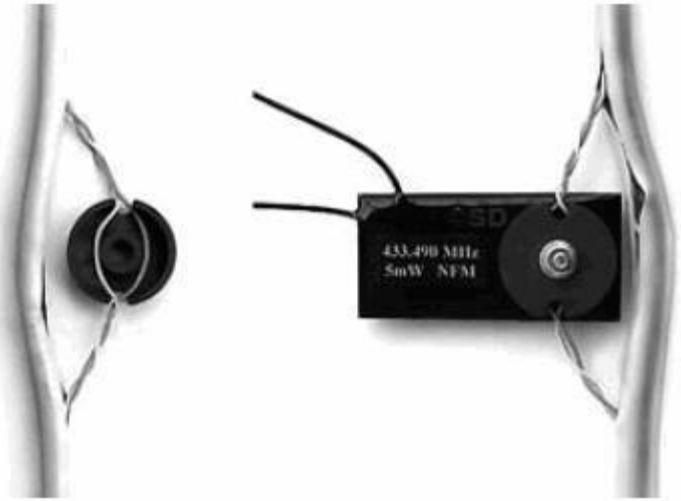
1. Устройства съёма информации в виде “отдельного модуля”, подключённые к телефонной линии “явным образом”: телефонный адаптер, индуктивный съёмник или “радиозакладка”, которая “висит на проводах”. Данные устройства могут быть легко обнаружены при внимательном осмотре абонентского участка телефонной линии, так как визуально они представляют собой *“подозрительный предмет непонятного назначения”*.

2. Устройства съёма информации, установленные внутри телефонного аппарата или закамуфлированные под типовые элементы телефонной сети: телефонная розетка, переходник, “разветвитель” и т.д. Обнаружить *(“идентифицировать”)* такие устройства намного сложнее – это может сделать только подготовленный человек, хорошо разбирающийся в устройстве телефонного оборудования – *а в ряде случаев даже он не сможет этого сделать без специального поискового оборудования*.

Примеры телефонных радиозакладок, подключаемых к телефонной линии на абонентском участке.



Телефонная радиозакладка, установленная в телефонной розетке



Подключение телефонной радиозакладки к линии с использованием индукционного датчика

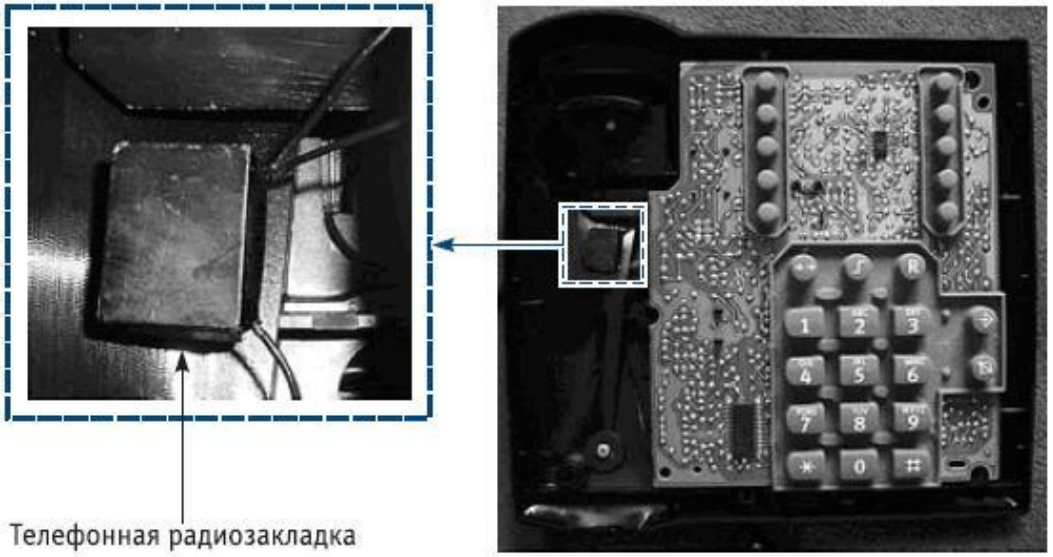
Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Примеры телефонных радиозакладок, устанавливаемых внутри абонентского оборудования.

“Радиозакладка” выполнена в виде “отдельного модуля”, но для её обнаружения нужно не только уметь разобрать телефонный аппарат – *что само по себе не так просто*, но и хорошо знать его устройство.

Как было сказано ранее: человек, не имеющий специальной подготовки, в большинстве случаев не поймёт, что это – “закладка”.

Телефонная радиозакладка, установленная в трубке телефонного аппарата



Телефонная радиозакладка, установленная в корпусе телефонного аппарата

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Примеры профессиональных телефонных радиозакладок.

Особую сложность представляет поиск “закладок”, выполненных в виде типовых элементов телефонного оборудования – например, в виде обычного конденсатора.

Обнаружить такое изделие в ходе визуального осмотра может только хорошо подготовленный человек, который разбирается в элементной базе радиоэлектронной аппаратуры и знает устройство соответствующего телекоммуникационного оборудования.

http://bugspy.narod.ru/index.files/stran/Spetstechnika/telobsh.html

Пример устройства, предназначенного для контроля речевой информации, которое “запитывается” от телефонного оборудования.

www.endoacustica.com

В большинстве случаев, характерных для “коммерческо-частного сектора”, данные изделия представляют собой радиомикрофон, установленный внутри телекоммуникационного оборудования или подключённый к телефонной линии, от которой он “запитывается”.

Внешне данные устройства могут быть выполнены как в виде “отдельного модуля”, так и быть закамуфлированы под различные “типовые” элементы – например, конденсатор или телефонную розетку.

Форум на Analitika.info → Противодействие техническим средствам шпионажа. Поисковые мероприятия → О камуфляже

09.09.2010 14:26:52

Сообщение от **nemo**

О камуфляже

К вопросу о том - надо ли проверять нелинейником раскрытую вручную телефонную розетку?
Попалась разок в руки очень достойно сделаная (однозначно заводская) телефонная розетка советского стандарта с двойным дном. Причем ее основание было толще обычного на пару миллиметров и в глаза не бросалось. В пустоте - комбинированная закладка на 140 МГц. Антенна - само собой телефонная линия. Контакты к ней подпаяны с внутренней стороны и не видны абсолютно. Нашли нелинейником NR-900M

Проводные системы, состоящие из “основного” электронного модуля – *микрофона или камеры*, соединённого с проводной линией *(кабелем)*.

Различные проводные системы аудио- и видеоконтроля достаточно широко используются в “коммерческо-частном секторе” – в основном данная угроза характерна для “чужой территории” или “арендованной территории”, но в некоторых случаях она может быть реализована злоумышленниками и на “вашей территории”.

В случае проводных систем съёма информации возможны два основных варианта:

- во-первых, для передачи информации может использоваться специально проложенный кабель, который “жёстко” связан с системой съёма информации и является её составной частью – это “классический” вариант;

- во-вторых, передача информации может осуществляться по “штатным” кабелям, имеющимся в помещении: речь идёт как о кабелях электросети, так и о кабелях слаботочных систем *(сигнализация, телефония, оповещение, LAN и т.п.)* – при этом, некоторые устройства съёма информации могут быть подключены не только к “свободным парам” этих кабелей, но и к “рабочим” проводам.

Как правило, **специально проложенные кабели** прокладываются за плинтусами, дверными наличниками, декоративными панелями и другими конструктивными элементами, которые являются “естественным прикрытием”. Кроме того, они могут быть проложены за подвесным потолком, в вентиляционных каналах и шахтах и других конструктивных полостях, имеющихся в помещении.

Проводные системы, состоящие из “основного” электронного модуля – *микрофон или камера*, соединённого с проводной линией *(кабелем)*.

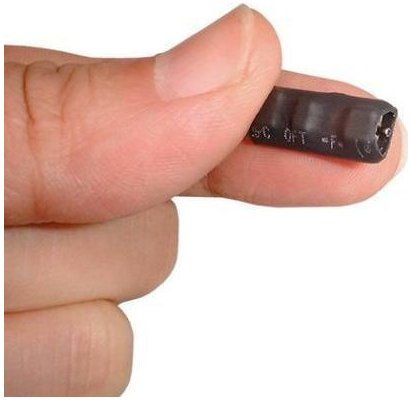
Обнаружение проводных систем съёма информации в ходе проведения ***визуального осмотра может быть весьма проблематичным*** *– всё зависит от конкретной ситуации.*

В ряде случаев проводной микрофон или видеокамера могут быть обнаружены достаточно легко при тщательном визуальном осмотре помещения: как непосредственно по их “внешнему виду” – *т.е. будет обнаружен сам “основной” электронный модуль (микрофон или камера)*, так и по наличию в помещении “непонятного кабеля”, который “приведёт” к микрофону или камере.

В то же время, если проводная система имеет “глубокий камуфляж” – *например, микрофон (камера) и соединительный кабель “замурованы” в ограждающих конструкциях помещения* – то обнаружить их без специального поискового оборудования *(а иногда даже при его наличии)* **практически невозможно**.

При осмотре “штатных” кабелей слаботочных систем, к которым могут быть подключены микрофон или камера, тоже есть много “нюансов”. Поэтому если визуальный осмотр проводит человек, не знакомый с “кабельными делами” – например, “личник”, которому поручили заниматься защитой информации, то для осмотра “штатных” кабелей целесообразно привлечь и обслуживающего их профильного специалиста из подразделения информационных технологий.

Примеры специальных проводных микрофонных систем.

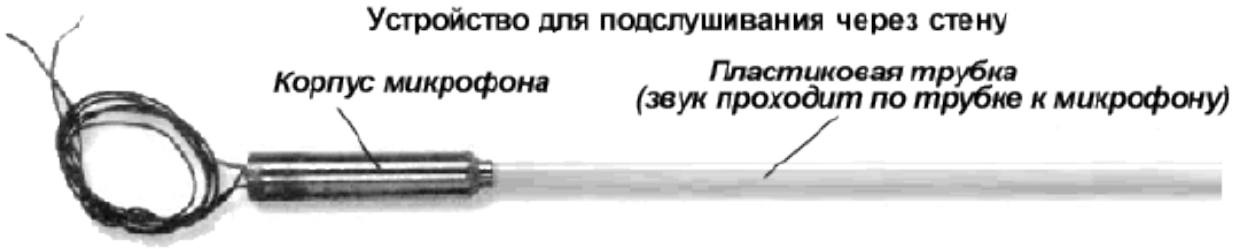


www.pki-electronic.com/products/audio-surveillance-equipment/

www.optoacoustics.com/sites/default/files/documents/optimic_brochure_2009_lite.pdf

Проводные микрофонные системы могут быть выполнены как на основе “классического” кабеля, так и с использованием оптоволокна.

Примеры проводных микрофонных систем, использующих “игольчатые” микрофоны.



При использовании так называемых “игольчатых” микрофонов злоумышленнику не требуется непосредственное проникновение в “нужное” помещение для их установки – достаточно наличия отверстия малого диаметра в ограждающих конструкциях *(стенах, полу или в потолке)*.
Если злоумышленник действует грамотно, то в большинстве случаев обнаружить такой микрофон в ходе визуального осмотра практически невозможно.

Для “коммерческо-частного сектора” это достаточно редкая угроза, но в ряде случаев её тоже надо иметь ввиду.

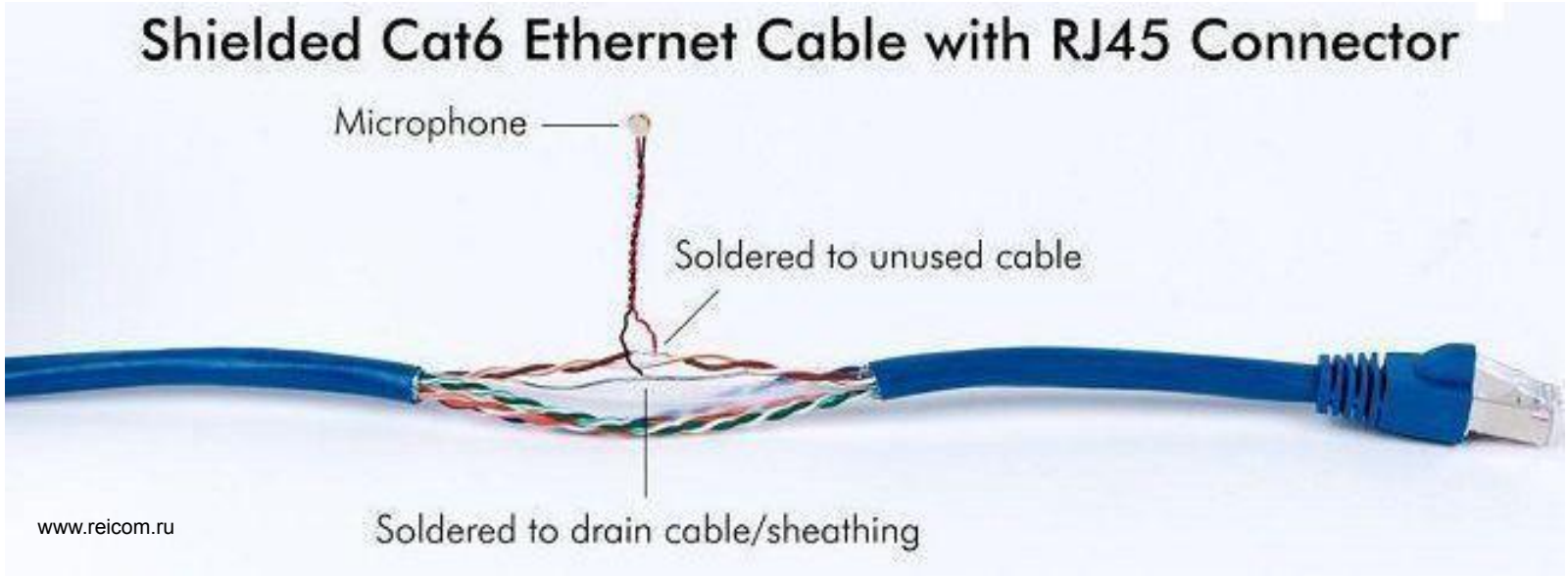
www.pki-electronic.com/products/audio-surveillance-equipment/needle-microphone-with-amplifier-2/

Примеры проводного микрофона и проводной видеокамеры, имеющих “глубокий камуфляж”.

В случае “глубокого камуфляжа” проводные системы могут быть “замурованы” в ограждающих конструкциях. Обнаружить такие устройства съёма информации без специального поискового оборудования практически невозможно.

В ряде случаев такие системы не получится обнаружить даже при наличии оборудования.

Пример микрофона, подключённого к “штатному” кабелю типа “витая пара”.



В некоторых случаях для передачи информации могут быть использованы “штатные” кабели различных “слаботочных” систем, проходящие через помещение – например, микрофон может быть подключён к незадействованным парам кабелей системы ОПС, телефонии, LAN и т.д.

*Как было ранее сказано, если вопросами защиты информации в компании поручено заниматься человеку, не разбирающемуся в “кабельных делах” – например, одному из “личников”, то визуальный осмотр “штатных” кабелей целесообразно (а точнее говоря – **необходимо**) проводить совместно с обслуживающим их связистом или сотрудником подразделения информационных технологий.*

Устройства “бытового назначения”, которые в ряде случаев могут быть использованы злоумышленниками для съёма информации.

В некоторых случаях в качестве устройства съёма информации может быть использовано какое-либо “бытовое устройство”, не имеющее каких-либо специальных “доработок”, которое находится в помещении.
В первую очередь речь идёт о различного рода включённых беспроводных устройствах связи, которые злоумышленник может оставить в помещении.

Самый “простой” вариант – это мобильный телефон или “Bluetooth-наушник”, находящиеся в помещении и работающие “на передачу”.
Существует много других устройств, которые могут быть использованы злоумышленниками с этой же целью и могут представлять реальную угрозу – *в частности, речь идёт об устройствах “радио-няня” (аудио и видео)*.

Данные устройства достаточно легко обнаружить при проведении тщательного визуального осмотра помещения – хотя внешне они представляют собой “обычное устройство радиосвязи”, но ***необходимо разбираться откуда они здесь взялись*** *и кому принадлежат.*
Этот момент касается любых телекоммуникационных устройств, находящихся в помещении.

Примеры “штатных” Bluetooth–устройств, которые могут быть использованы злоумышленником в качестве “закладки”.

Речь идёт именно о “штатных” Bluetooth-устройствах, которые “тупо” оставлены в помещении и работают на “передачу”.

Специальные закладные устройства, работающие на основе Bluetooth-технологии – это совсем другое дело.

Пример “радио-няни” и радиостанции с функцией “радио-няня” .

Радионяня Ramili Baby RA400 Black

Радионяня от английской компании Ramili Baby RA400, которая работает на современной технологии передачи звука на большом расстоянии. Радионяня Ramili RA400 оснащена всеми необходимыми функциями, которые позволяют без затруднений обеспечивать контроль за ребенком в больших квартирах или в домах.

Радионяня оснащена системой активации при обнаружении плача (VOX) и незамедлительно включает звук или подает тревожный сигнал на родительском блоке в том случае, если звук выключен, когда малыш расплакался. Кроме того, радионяня непрерывно мониторит происходящее в детской комнате и включает трансляцию на родительском блоке, несмотря на то, что в детской комнате тихо. Таким образом устройство самостоятельно обеспечивает непрерывный контроль. По требованию родителей, нажав на кнопку обратной связи, можно самостоятельно услышать звук из детской.

Рация Switel WTF778 (10 км, функция радионяни, «Беби мониторинг»)

Рация Switel WTF778 с функциями VOX и «Беби мониторинг» от Швейцарского производителя высококачественной электроники Telgo AG. Такая рация работает аналогично радионяне с функцией автоматической активации при плаче, обеспечивая качественную, устойчивую связь на очень большом расстоянии (до 10 км). Принцип работы рации с функцией радионяни Switel WTF778 заключается в следующем: на одном из двух блоков вы включаете функцию «Беби мониторинг», активируется система распознавания звука, отключаются все функции рации, кроме обнаружения плача ребенка или громкого звука. Если вдруг малыш заплачет или будет обнаружен звук (шум), громкость которого превышает установленный вами уровень чувствительности, то рация автоматически активируется и начнет передачу на тот блок, который находится у родителей.

Угроза утечки информации за счёт “физических особенностей” некоторого “штатного” оборудования, находящегося в помещении.

Речь идёт о так называем “акустоэлектрическом преобразовании”, а конкретнее о возможной утечке за счёт “микрофонного эффекта” и “ВЧ-навязывания”.

Данные угрозы достаточно подробно рассмотрены в презентации “*Технические каналы утечки акустической информации*”.

Эти угрозы очень “специфичны” *(хотя в ряде случаев достаточно реальны)* и **обнаружить их в ходе визуального осмотра помещения невозможно** – их поиском должен заниматься подготовленный человек, хорошо понимающий “физику” их возникновения и имеющий специальное поисковое оборудование.

В компаниях, где с защитой информации “всё по взрослому”, этот вопрос решается *(по крайней мере должен решаться)* соответствующим образом.

В то же время в большинстве реальных случаев – когда вопросы защиты информации возложены “по совместительству” на кого-то из сотрудников личной охраны, связистов или “компьютерщиков” – об этих вещах даже не подозревают. Как было сказано ранее, в этом случае сотрудник, отвечающий за защиту информации, **в принципе не сможет ничего сделать** – *он не имеет нужной подготовки и необходимого оборудования*, но он должен хотя бы иметь представление о таких угрозах.

Съём информации за счёт “штатных” возможностей и “дополнительных” функций средств вычислительной техники и телекоммуникационного оборудования, находящихся в помещении.

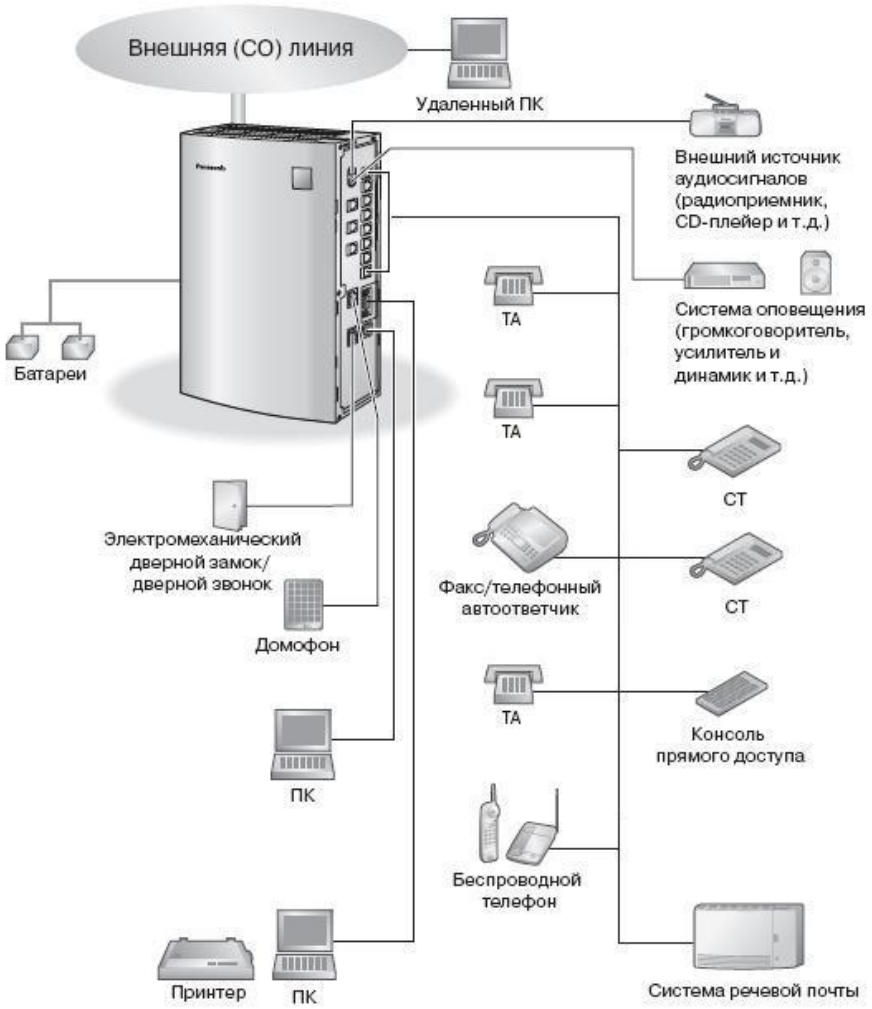
Речь идёт о некоторых “штатных” возможностях и так называемых “дополнительных” функциях, которые имеются в средствах вычислительной техники и в некоторых моделях телекоммуникационного оборудования. Необходимо отметить, что данные функции являются именно “штатными” – они чётко прописаны в “Инструкции по эксплуатации” на эти устройства и, при определённом стечении обстоятельств, ими может воспользоваться грамотный злоумышленник как для перехвата информации, циркулирующей в телекоммуникационных сетях, так и для получения аудио- и видеоинформации из помещений, в которых находятся соответствующие абонентские устройства: *компьютер, телефонный аппарат, автоответчик и т.д*.

Данные угрозы достаточно подробно рассмотрены в презентациях “*Технические каналы утечки акустической информации*” и “*Технические каналы утечки информации, передаваемой по каналам связи*”.

Ещё раз нужно отметить, что речь идёт именно о “штатных” функциях: *“Автоматический ответ”, “Вклинивание в разговор”, “Room Monitoring” и т.д*.

Для выявления этих угроз необходима плановая совместная работа подразделения информационных технологий и подразделения, отвечающего за вопросы ТЗИ, **сотрудники которых должны иметь необходимую подготовку**.

Примеры “дополнительных” функций, имеющихся в некотором телекоммуникационном оборудовании (мини-АТС).



- Большинство современных мини-АТС позволяют осуществлять скрытый контроль ведущихся по ним телефонных переговоров: *прослушивание в режиме реального времени или их запись*. Например, такая возможность реализуется за счёт функции “**Вторжение в разговор**” и функции “**Автоматическая запись в систему голосовой почты**”, которые “активируются” с помощью соответствующей настройки (программирования) АТС.
- Кроме того, многие современные мини-АТС позволяют осуществлять скрытый контроль за акустикой помещений, в которых установлены телефонные аппараты: так называемая функция **“Room Monitoring”** – одна из “дополнительных” функций мини-АТС. Данная возможность реализуется за счёт использования так называемых “системных телефонов” (СТ) и их соответствующей настройки *(программирования)* – образно говоря, она аналогична использованию закладных устройств типа “телефонное ухо”.

Съём информации за счёт “программных закладок”, внедрённых в вычислительную технику и телекоммуникационное оборудование.

Очень серьёзная угроза связана с применением т.н. “программных закладок”, которые могут быть внедрены злоумышленником в средства вычислительной техники и в некоторые модели телекоммуникационного оборудования.
В этом случае ваш “родной” компьютер, “планшет”, смартфон и т.п. переходит под дистанционное управление злоумышленником и фактически становится устройством съёма информации – причём **для получения информации используются его “штатные” микрофон и видеокамера**.

Данные угрозы достаточно подробно рассмотрены в презентациях “*Технические каналы утечки акустической информации*” и “*Технические каналы утечки информации, передаваемой по каналам связи*”.

Естественно, что ***в ходе проведения визуального осмотра помещения невозможно обнаружить угрозы****, связанные с “программными закладками”, внедрёнными в СВТ и телекоммуникационное оборудование (в том числе и т.н. “телефоны-шпионы”)*.
Для выявления этих угроз необходима плановая совместная работа подразделения информационных технологий и подразделения, отвечающего за вопросы ТЗИ, **сотрудники которых должны иметь специальную подготовку**.

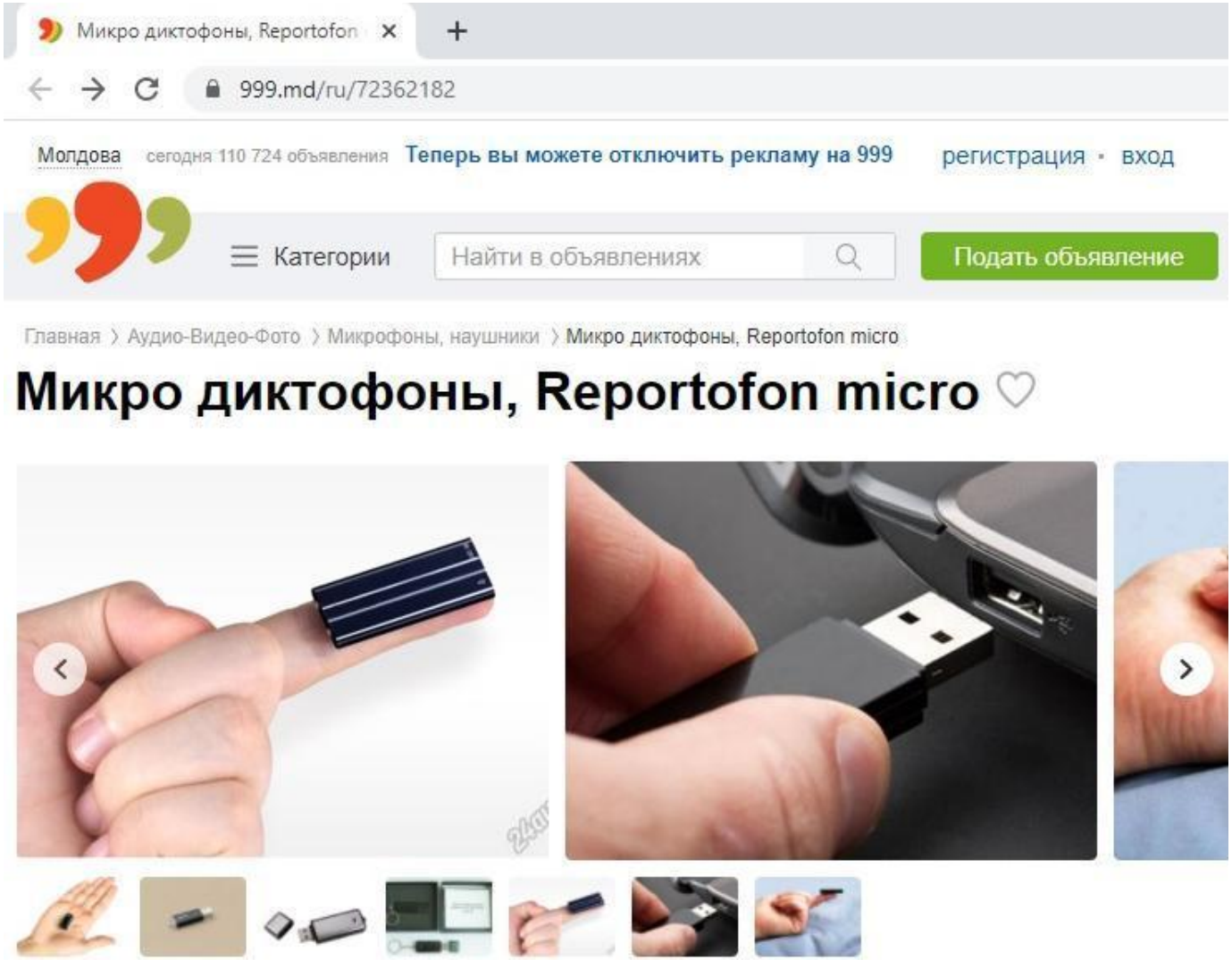
Принцип работы “Телефонов-шпионов” (Spy Phones).

Spy Phone (“телефон-шпион”) – это устройство, выполненное на базе сотового телефона или смартфона, на который установлено специальное программное обеспечение.

Профессиональный “телефон-шпион” позволяет полностью контролировать практически всю информацию, “проходящую” через данный мобильный телефон: *сообщения и телефонные разговоры – как “обычные”, так и передаваемые по различным “мессенджерам”, данные из памяти телефона и т.д*.

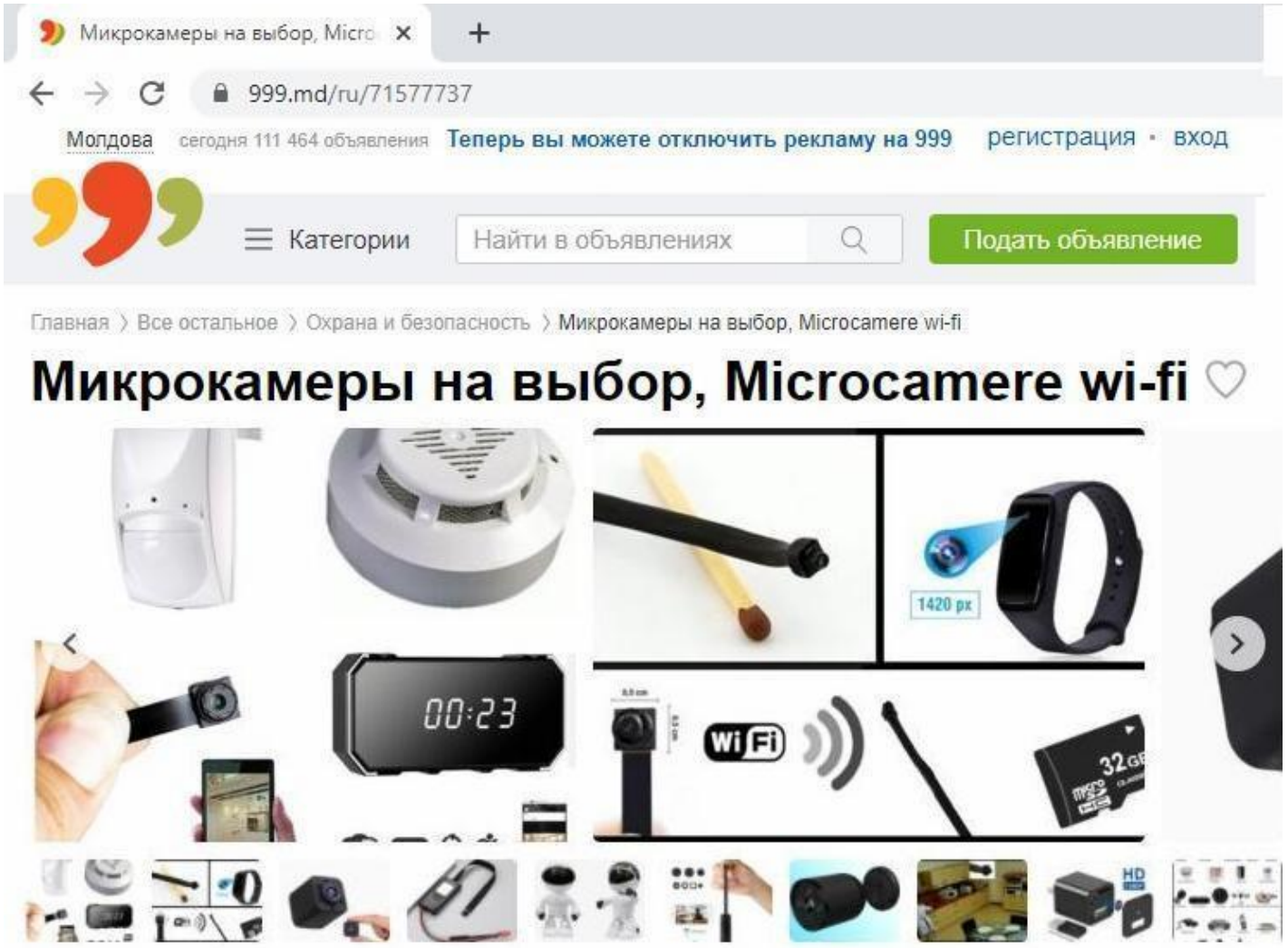
Кроме того, данное устройство позволяет задействовать “штатные” микрофон и камеру телефона для перехвата аудио- и видеоинформации – *таким образом телефон практически становится аудио- и видео- “закладкой”*.

Пример диктофонов, предлагаемых на молдавском рынке.



Есть разные модели: Микро диктофоны, диктофоны флешки с функцией VOX (активация голоса), Видео флешки.

Пример видеокамер, предлагаемых на молдавском рынке.



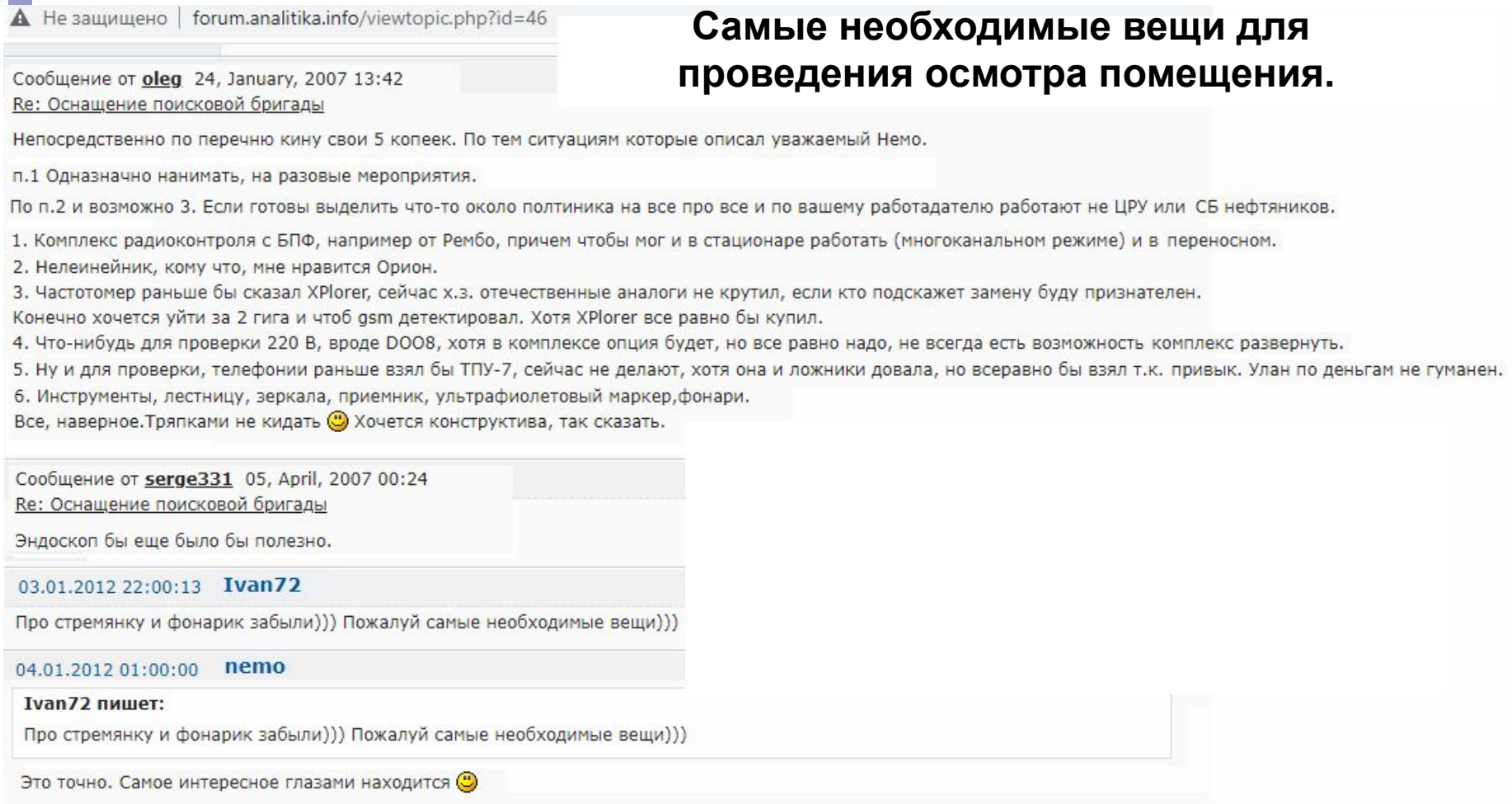
Ещё раз о техническом оснащении “поисковика” .

Как было сказано ранее, в абсолютном большинстве случаев, характерных для “молдавской действительности”, в компании нет отдельного подразделения, занимающегося технической защитой информации. Поэтому, данные задачи – *в частности поиск возможно внедрённых устройств съёма информации* – как правило, возложены “в нагрузку” на сотрудника личной охраны, не имеющего специальной подготовки в данной области. Естественно, что в этом случае о приобретении какого-либо специального поискового оборудования речь даже не идёт.

Как было отмечено, в этом случае **основной упор надо делать на тщательный визуальный осмотр помещения**, который достаточно эффективен для поиска большинства устройств съёма информации, используемых в “коммерческо-частном секторе” *(в первую очередь речь идёт о наиболее распространённых “заносных” закладных устройствах различного типа, не имеющих “глубокого камуфляжа”)* – естественно, если осмотр проводится адекватным и думающим человеком.

В то же время, существует ряд самых обычных технических средств, которые **необходимы** для проведения визуального осмотра помещения.

Самые необходимые вещи для проведения осмотра помещения.



Не защищено | forum.analitika.info/viewtopic.php?id=46

Сообщение от **oleg** 24, January, 2007 13:42
Re: Оснащение поисковой бригады

Непосредственно по перечню кину свои 5 копеек. По тем ситуациям которые описал уважаемый Немо.

п.1 Однозначно нанимать, на разовые мероприятия.

По п.2 и возможно 3. Если готовы выделить что-то около полтиника на все про все и по вашему работадателю работают не ЦРУ или СБ нефтяников.

1. Комплекс радиоконтроля с БПФ, например от Рембо, причем чтобы мог и в стационаре работать (многоканальном режиме) и в переносном.
2. Нелеинейник, кому что, мне нравится Орион.
3. Частотомер раньше бы сказал XPlorer, сейчас х.з. отечественные аналоги не крутил, если кто подскажет замену буду признателен.
Конечно хочется уйти за 2 гига и чтоб gsm детектировал. Хотя XPlorer все равно бы купил.
4. Что-нибудь для проверки 220 В, вроде DOO8, хотя в комплексе опция будет, но все равно надо, не всегда есть возможность комплекс развернуть.
5. Ну и для проверки, телефонии раньше взял бы ТПУ-7, сейчас не делают, хотя она и ложники довала, но всеравно бы взял т.к. привык. Улан по деньгам не гуманен.
6. Инструменты, лестницу, зеркала, приемник, ультрафиолетовый маркер,фонари.
Все, наверное.Тряпками не кидать Хочется конструктива, так сказать.

Сообщение от **serge331** 05, April, 2007 00:24
Re: Оснащение поисковой бригады

Эндоскоп бы еще было бы полезно.

03.01.2012 22:00:13 **Ivan72**

Про стремянку и фонарик забыли))) Пожалуй самые необходимые вещи)))

04.01.2012 01:00:00 **nemo**

Ivan72 пишет:

Про стремянку и фонарик забыли))) Пожалуй самые необходимые вещи)))

Это точно. Самое интересное глазами находится

По поводу **“самых необходимых вещей”** – абсолютно согласен с Ivan72 и nemo: **фонарик** и **стремянка**, ну и **отвёртка** ещё.

Естественно, что эти три “основных орудия производства” должны прилагаться к умелым рукам, внимательным глазам и думающей голове.

Фонарь.

Фонарь, используемый при проведении специального обследования помещения, должен на только обеспечивать необходимую подсветку, но и иметь небольшие габариты и надёжную конструкцию – учитывая, что в ходе работ он будет эксплуатироваться в “достаточно сложных” условиях – пыль, влажность, механические воздействия. Желательно, чтобы фонарь имел возможность регулировки “дальности подсветки” и “размера светового пятна”.

Примеры фонарей.

Лестница-стремянка.

Лестница должна быть надёжной, лёгкой и удобной для перемещения одним человеком. Высота стремянки должна обеспечивать свободный доступ к потолкам проверяемого помещения.

Набор отвёрток.

При проведении осмотра помещения отвёртка нужна как для того, чтобы “подковырнуть” что-нибудь *(съёмную крышку, плинтус или наличник)*, так и для того, чтобы “разобрать” *(“открутить”)* что-нибудь *(розетку, удлинитель, легкоразборный элемент интерьера и т.д.)*.

Поэтому нужно иметь несколько отвёрток: одну для “грубой” работы и еще две *(“плоскую” и “крестовую”)* для “откручивания”. Отвёрток может быть и больше – вопрос в том, будут ли они все использоваться при работе.

Досмотровый инструмент.

Кроме **фонаря** и **отвёртки** *(которые являются **обязательными**)* при проведении осмотра помещения могут быть полезны и другие инструменты и приборы – главное, чтобы проводящий осмотр умел ими грамотно пользоваться.

Для осмотра труднодоступных мест – *различные конструктивные полости, щели, воздуховоды и т.д.* – очень полезными будут **досмотровые зеркала** и **эндоскоп**. Но тут всё уже зависит от финансирования – например, цена более-менее качественного эндоскопа может составлять от 1000 USD и выше.

Есть ещё **специальные телевизионные досмотровые системы**, но у них уже совсем другая цена – *по сравнению с досмотровыми зеркалами и эндоскопами*.

Существуют уже готовые “Комплекты досмотрового инструмента”, в состав которых входят различные инструменты и приборы, используемые для визуального осмотра помещений и физического поиска устройств съёма информации *(но у них тоже “совсем другая цена”)*.

Нужно **чётко понимать** и **постоянно помнить**, что всё это – только “инструментарий”, который может помочь при поиске, но не сможет *“сделать чуда”* и *“сам что-то найти”*.

А **главное при осмотре помещения** – это глаза, которыми надо “вживую” всё осмотреть, и руки, которыми надо “вживую” всё “прощупать”.

Набор досмотровых зеркал.

Набор досмотровых зеркал представляет собой телескопическую “штангу”, к которой крепятся сменные зеркала различного размера и формы.
В комплект так же может входить фонарь для подсветки.

“Малые” досмотровые зеркала.

www.novocom.ru

www.reiusa.net

Гибкие видеоэндоскопы.

Жёсткий эндоскоп *(бороскоп)*.

www.reiusa.net

Телевизионные досмотровые системы.

www.reiusa.net

www.suritel.ru

Комплект досмотрового инструмента “Калейдоскоп-П2”.

Комплект досмотрового инструмента ОТК-4000.

Ещё раз о необходимости “проявлять разумную инициативу”.

Как было сказано ранее, если в компании нет “штатного” подразделения ТЗИ, занимающегося поиском возможно внедрённых устройств съёма информации, а эти вопросы возложены в качестве “нагрузки” на кого-нибудь из “лички”, то в большинстве случаев оснащение каким-либо специальным поисковым оборудованием практически отсутствует и основной упор при поиске надо делать на **визуальный осмотр помещения**.

Но **всегда нужно помнить** о необходимости “проявлять **разумную** инициативу” и стараться максимально использовать все имеющиеся “подручные” средства.

Часто бывает, что финансирование “по линии поисковой техники” в компании практически отсутствует, но при этом финансирование *(оснащение)* по линии физической защиты и антитеррора вполне приличное: имеются не только металлодетекторы и досмотровые зеркала, но в **некоторых редких случаях** даже стационарные рентгеновские установки (“туннельного” или “камерного” типа) – как правило, они находятся на входе в здание и используются для досмотра личных вещей посетителей и поступающей корреспонденции.

Вся **эта техника может и должна быть задействована** “сотрудником-поисковиком” для решения вопросов, связанных с защитой информации – главное грамотно и эффективно её использовать.

Портативные *(ручные)* металлодетекторы.

Портативные металлодетекторы могут быть очень полезны при поиске устройств съёма информации *(в дополнении к визуальному осмотру помещения)*.
Как было сказано ранее, очень часто денег на специальную поисковую технику не дождёшься – *например, о покупке НЛ даже речи быть не может.*
В то же время, металлодетектор всегда есть у охраны в большинстве компаний. Сотруднику, отвечающему за проведение “поисковых работ”, нужно просто уметь **грамотно его использовать** в “своих интересах”.

Стационарные рентгенотелевизионные досмотровые установки.

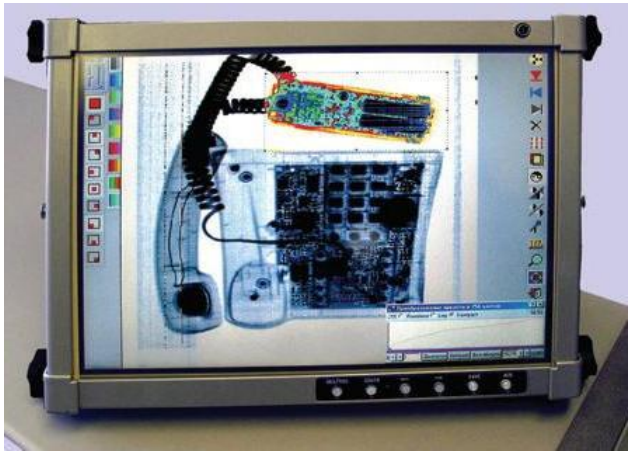
В некоторых **очень редких случаях** может быть ситуация, когда *“денег на поисковую технику нет” (как это обычно бывает)*, но в компании имеется стационарная рентгенотелевизионная установка (*“туннельного”* или *“камерного”* типа), используемая для “вопросов антитеррора”: проверка ручной клади посетителей, контроль почтовой корреспонденции и т.п.

В этом случае сотрудник, отвечающий за защиту информации, должен максимально использовать данную возможность для проведения исследования предметов интерьера, которые могут быть проверены с помощью такой установки.

Для грамотной работы данный сотрудник должен пройти соответствующую подготовку.

www.rapiscansystems.com

Пример стационарной рентгенотелевизионной досмотровой установки.



В отличие от портативных установок, которые находятся “на вооружении” у профессиональных “поисковиков”, стационарные рентгенотелевизионные установки могут использоваться в самых различных организациях *(компаниях)*.

Важным преимуществом стационарных установок является их практически полная радиационная безопасность.

В то же время, у них есть ограничение на размер проверяемых предметов, связанное с габаритами камеры *(“туннеля”)*.

Некоторые “общие” моменты, касающиеся использования стационарной рентгенотелевизионной досмотровой установки.

Как было сказано ранее, наличие в компании рентгенотелевизионной досмотровой установки – *например, по линии антитеррора* – это большая редкость для молдавского “коммерческо-частного сектора” *(можно сказать “единичные случаи”)*.

Если же такая возможность всё-таки есть, то нужно иметь ввиду несколько моментов, связанных с использованием данного оборудования для проверки различных предметов на наличие в них средств съёма информации.

Одно дело когда будет проводиться проверка каких-либо предметов, в которых по определению не должно быть электронных элементов: авторучек и маркеров, мягких игрушек, статуэток, книг и т.д. – там всё “относительно просто” и на экране установки можно будет увидеть на фоне однородной структуры какие-то “непонятные элементы”, которых там не должно быть.

И совсем другое дело – это проверка устройств, содержащих “штатную” электронику: телекоммуникационное оборудование, электронные игрушки, электромеханические и электронные часы и т.д. В этом случае, увидеть на фоне “штатной” электроники элементы закладного устройства *(особенно “заводского” изготовления)* сможет только опытный специалист и то, как правило, при наличие у него так называемой *“базы рентгенограмм эталонных образцов электронного оборудования”*.

Это я к тому, что здесь всё не так просто – *см. фото на предыдущем слайде*.

Немного о проведении визуального осмотра помещения.

Далее будут рассмотрены некоторые основные моменты, связанные непосредственно с визуальным осмотром как конструктивных элементов проверяемого помещения, так и находящихся в нём предметов интерьера.

Хочу подчеркнуть, что это не какие-то *“тайные тайны”* и *“секретные секреты”*, в существовании которых уверены многие граждане и *“диванные эксперты”*, насмотревшиеся *“шпионских фильмов”*.

Всё, о чём будет рассказано далее, это **элементарные вещи, которые может выполнить любой человек** – *если, конечно, у него есть думающая голова, внимательные глаза и более-менее умелые руки*.

В то же время, необходимо отметить, что всё это – **только небольшая часть** той работы, которая должна проводиться при **настоящей проверке** помещения.

Ещё раз повторю: речь пойдёт о проведении визуального осмотра помещения, который возможен без использования какой-то специальной поисковой техники.

В то же время, будут упоминаться различные “обычные” средства – например, отвёртка или фонарь, которые имеются у каждого.

Так же будут упоминаться некоторые технические средства, которые могут быть без проблем приобретены *(например, досмотровые зеркала)* или которые могут иметься в компании *(например, портативные металлодетекторы)*.

Некоторые “общие” моменты, касающиеся проведения визуального осмотра помещения.

Важным моментом, связанным с проведением визуального осмотра помещения, является, образно говоря, “общетехническая” подготовка “поисковика”.

Имеется ввиду, что в ходе проведения осмотра всегда возникает необходимость что-то разобрать, открутить или отсоединить – *естественно, что потом всё надо обратно “собрать, прикрутить и присоединить”*.

Понятно, что какие-нибудь сложные “манипуляции” – *типа разборки телекоммуникационного оборудования, средств вычислительной техники, бытовой электронной техники и т.п.* – должны проводиться только специально обученным “поисковиком” или привлекаемым для этих работ сотрудником подразделения информационных технологий.

Но есть элементарные вещи, которые должен уметь делать любой мужчина: *снять дверной наличник, “вскрыть” пластиковый кабель-канал или плинтус, отсоединить легкосъёмный элемент мебели или декоративную панель, разобрать электроудлинитель, “тройник” или настольную лампу и т.п.*

Да, для этого требуются определённые навыки, но ничего сложного там нет.

*Главное, чтобы не получилось “разобрать” проверяемый предмет так, как кузнец Степан разобрал карету графа Калиостро в “**Формуле любви**”.*

Некоторые “общие” моменты, касающиеся проведения визуального осмотра помещения.

Визуальный осмотр помещения должен проводиться “системно” – т.е. по определённой схеме, предусматривающей **полный охват** не только **всех конструктивных элементов** проверяемого помещения, но и **всех предметов**, находящихся в данном помещении.

*Здесь очень уместен диалог из хорошего фильма “**Если верить Лопотухину**”:*

- Значит ты, Петров, будешь двигаться по меридианам: с севера на юг. Понял? Давай! А ты, Павлов, будешь двигаться по параллелям: с запада на восток. Усёк?

- Слушай, Шафиров, а ты как пойдёшь?

- А я пойду по синусоиде!

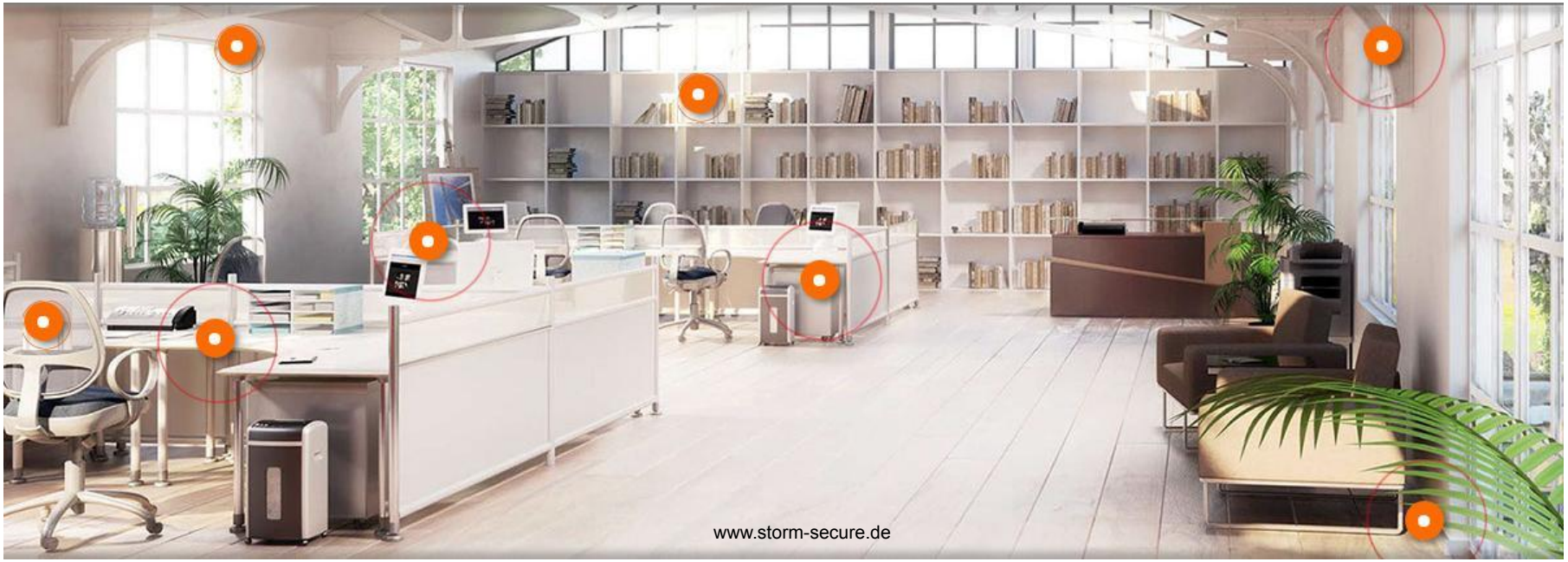
- По синусоиде???

- Да, по синусоиде. Помните: мы должны изучить каждый клочок земли на этом участке, не пропустить ни одного квадратного сантиметра!

Так что в принципе “поисковик” может двигаться хоть по *“кубической параболе”* – **главное, чтобы “не было пропущено ни одного квадратного сантиметра”**.

Однако, при проведении визуального осмотра помещения лучше выбрать более простую *(но не менее надёжную)* “траекторию движения” – например, осмотр можно проводить от входной двери против часовой стрелки и от стен к центру помещения, охватывая все уровни *(от пола до потолка)*.

Немного о возможных местах установки устройств съёма информации.



Устройства съёма информации могут быть установлены в самых различных местах. При этом, как уже говорилось, есть принципиальный момент, связанный с особенностью работы средств видео- и аудиоконтроля, который влияет на их размещение и, соответственно, их поиск.

Видеокамера должна иметь “непосредственный выход” в помещение – её “зрачок” должен чётко смотреть в нужную сторону – *иначе камера ничего “не увидит”*.
Между объективом камеры и объектом съёмки не должно быть каких-либо преград.

Для **устройств аудиоконтроля** ситуация другая: совсем не обязательно, чтобы микрофон был направлен прямо на источник звука. Поэтому устройства аудиоконтроля могут быть установлены за различными “преградами”: в ящике стола, внутри дивана, под ковром, между стеной и плинтусом, за подвесным потолком и т.д.

Некоторые возможные места установки устройств съёма информации.

www.pimall.com

Осмотр дверей.

Двери *(вместе с дверной коробкой)* – это сложная конструкция, в которую могут быть внедрены различные средства съёма информации.

Причём для их установки в большинстве случаев не нужно что-то “долбить” или “сверлить”, а достаточно использовать уже имеющиеся “идеальные” места.

Очень часто при установке дверей между дверной коробкой и дверным проёмом в стене остаются большие щели, которые просто “закрывают” наличниками.

Иногда эти щели используют для прокладки штатных кабельных коммуникаций.

Кроме того, часто используются “полые” наличники со встроенным кабель-каналом.

В зависимости от конкретной конструкции дверей могут быть и другие “сюрпризы”, которыми может воспользоваться злоумышленник.

Осмотр дверей.

Прямо как в поговорке:

“***С такими “друзьями” нам не нужны враги***”.

Осмотр дверей.

Осмотреть дверь и дверную коробку, обращая особое внимание на “штатные” пазы и полости, которые могут в них быть.

Если есть возможность, то снять наличники и осмотреть пространство за ними. Если наличники закреплены “намертво”, то осмотреть щели за ними – *на сколько это возможно*.

Полые наличники со встроенным кабель-каналом открыть для осмотра обязательно.

Осмотр стен – у которых, согласно поговорки *“тоже могут быть уши”*.

Многие граждане твёрдо убеждены, что именно в стену “**должно быть что-то заложено**” – причём, как это “**что-то**” могло попасть в стену они не представляют, но уверены в том, что “оно” там есть.

Осмотр стен.

Каждое помещение имеет “свои” стены – *как по конструкции, так и по “загруженности” различными предметами интерьера*.
В ряде случаев “стена” (в прямом значении) может вообще “отсутствовать” – по всему периметру помещения установлена “встроенная” мебель.

Если *не рассматривать угрозу “глубокого камуфляжа” средств съёма информации*, то основное внимание при осмотре нужно обратить на наличие “посторонних предметов”, прикреплённых непосредственно к стене или к элементам интерьера, находящимся на ней.

Как было сказано ранее, установить закладное устройство в “самой стене” – *“замуровав” после этого стену* – это сложная процедура, которая требует длительного свободного доступа в нужное помещение и целой “команды” специалистов.

Осмотр стен *(общие моменты)*.

- В первую очередь необходимо отодвинуть от стен всю мебель – если это возможно. Если отодвинуть мебель от стены нельзя, то с помощью фонаря и зеркал (эндоскопа) осматривается пространство между мебелью и стеной.
- Одновременно с осмотром стен производится тщательный осмотр находящихся на них предметов интерьера и покрытий: полки, картины, зеркала, бра, ковры и т.д., которые по возможности должны сниматься. Внимательно осматриваются установленные на стенах датчики, телевизоры, кондиционеры и т.п. – *далее будет рассказано о некоторых особенностях осмотра "штатной электроники"*.
- Если стены закрыты декоративными панелями, то внимательно осмотреть их поверхности и места "стыков". Легкосъёмные панели снимаются для осмотра.
- Если стены оклеены обоями, то особое внимание нужно обратить на места их "стыков", вздутия, порезов и надрывов.
- При наличии в стенах каких-либо технологических ниш, закрываемых съёмными крышками, их необходимо открыть и осмотреть.
- Если вдоль стен проложены пластиковые кабель-каналы *(короба)*, то они осматриваются отдельно – *см. далее*.
- Производится осмотр электрических розеток и выключателей – *см. далее.*

Осмотр стен.

Даже на любой “простой” квартирной стене есть что осматривать: розетки, выключатели, бра, картины и фотографии *(в рамках и без)*, сувениры и т.д. – не говоря уже о самой стене и о пространстве между стеной и мебелью.

Да, это “рутинная” процедура, но её надо делать.

И “не расслабляться” типа: *“Да что там может быть? Это же стена!”*.

Осмотр стен – ***несколько примеров “явных проблем с обоями”, на которые надо обратить особое внимание при осмотре*****.**

Осмотр стен с использованием эндоскопа.

В случае “накладных” стен – *например, обшитых гипсокартоном или несъёмными декоративными панелями* – очень полезен будет эндоскоп (если он есть в наличии).

С помощью эндоскопа необходимо осмотреть пространство между *“основной”* и *“накладной”* стеной – *если есть возможность “попасть” туда*.

Пример осмотра предметов интерьера, находящихся на стене *(бра)*.

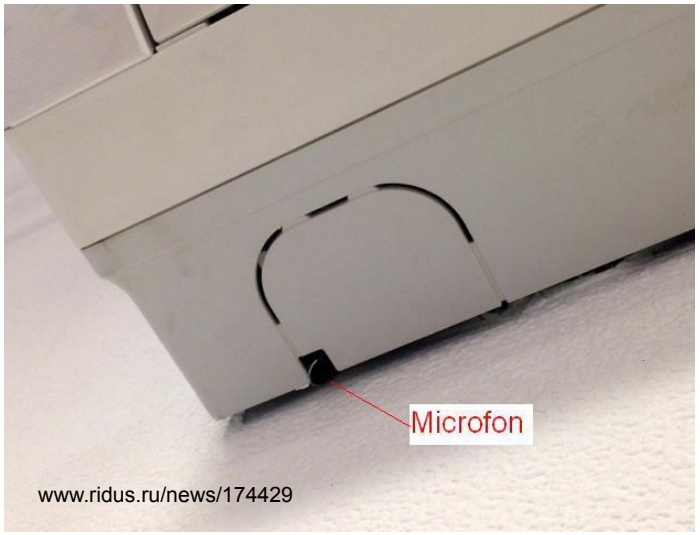
Настенные лампы *(бра)* и аналогичные изделия отключаются *(отсоединяются)* от сети, разбираются и осматриваются.

Пример осмотра предметов интерьера, находящихся на стене *(картины)*.

Картины снимаются со стены и внимательно осматриваются.
Особое внимание нужно обратить на раму и тыльную сторону картины.

При наличии портативного металлодетектора будет очень полезно проверить картину с его помощью.

Пример осмотра бытовой электроники, установленной на стене *(кондиционер)*.



*Все работы по установке, ремонту и техобслуживанию кондиционера должны обязательно “сопровождаться” **толковым** сотрудником компании.*

Устройства съёма информации могут быть как “встроены” в кондиционер – *как правило, “самостоятельно” злоумышленником*, так и быть просто “прикреплены” к его корпусу.

При осмотре кондиционера особое внимание необходимо обратить на его верхнюю часть *(пространство между кондиционером и потолком)* и на щели между кондиционером и стеной, а так же на доступные для осмотра внутренние полости. *При осмотре необходимо использовать фонарь и малое зеркало.*

Пример осмотра бытовой электроники, установленной на стене *(кондиционер)*.

Если в наличии имеется эндоскоп, то его нужно использовать для осмотра различных полостей, имеющихся в кондиционере.

При работе **соблюдать правила электробезопасности**.

Осмотр стен на “чужой территории”.

Как было сказано выше: “чужая территория” – это по определению “зона повышенной опасности” *(в плане возможного съёма информации)*.

При осмотре стен на “чужой территории” необходимо обратить внимание на такой нюанс, как возможность установки в них т.н. “прозрачных” зеркал или даже целых “прозрачных” зеркальных стен (потолков). Такая угроза может быть реализована “злоумышленниками-хозяевами” в любом “чужом помещении” – в том числе в гостиницах, *“банях”*, *“массажных кабинетах”* и т.п.

При проведении осмотра на “чужой территории” необходимо в обязательном порядке убедиться в “непрозрачности” зеркал:
в том, что зеркала не “встроены” в стену, а съёмные. Если же в проверяемом помещении имеется “зеркальная стена” (потолок), то это вообще должно “напрячь” и нужно разбираться с этим вопросом.

Осмотр окон.

С точки зрения проверки окно представляет собой целый комплекс “составляющих элементов”, каждый из которых требует внимательного осмотра: оконные рамы, оконный проём, подоконник, шторы *(жалюзи)* с элементами крепления и т.д.

Средства съёма информации могут быть как просто “прикреплены” к одному из “составных элементов” окна, так и “внедрены” в них – в том числе за счёт естественных пустот и особенностей конструкции.

Осмотр окон *(общие моменты)*.

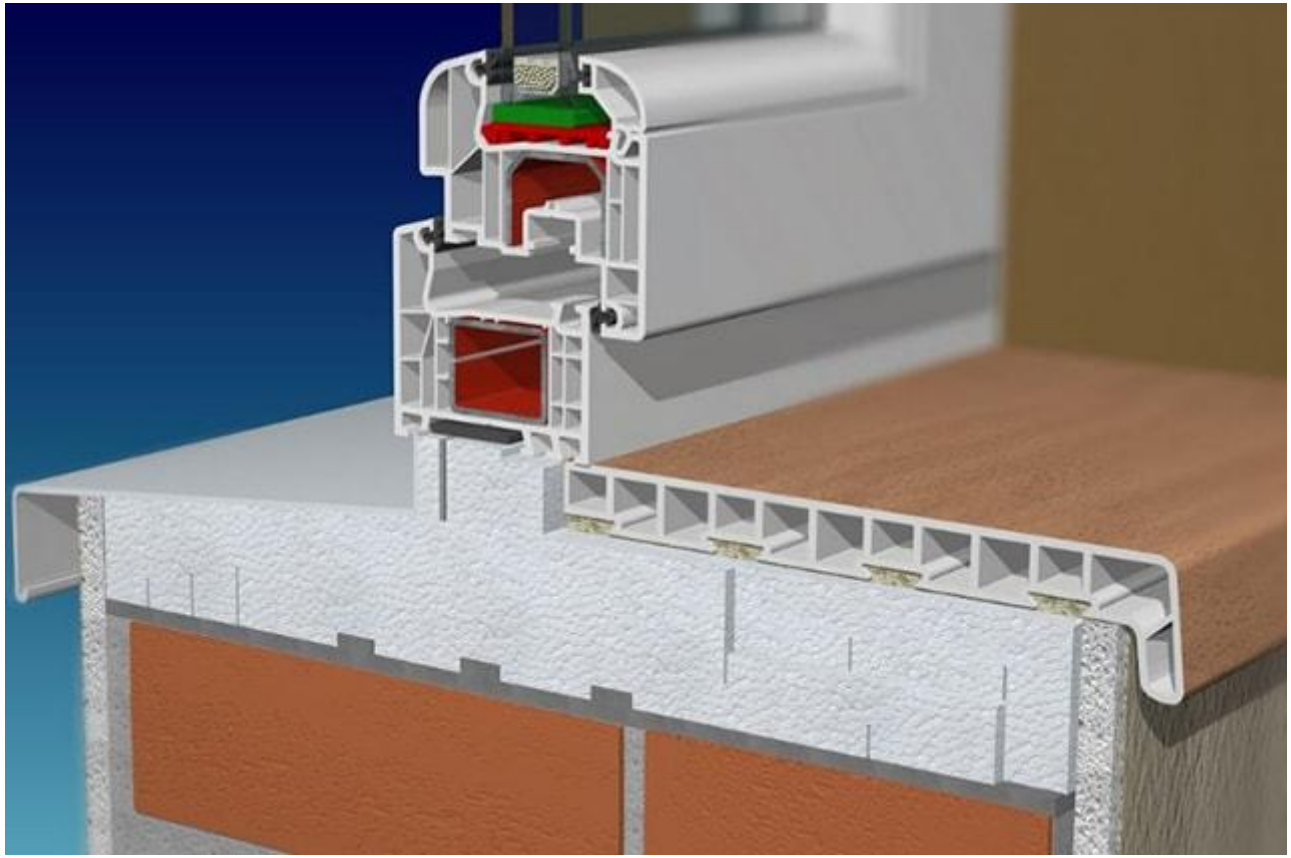
Поверхность подоконника *(особое внимание обратить на нижнюю часть)*, оконный проём *(т.н. “откосы”)* и оконные рамы внимательно осматриваются на наличие посторонних предметов.

Подоконник “прощупывается” на наличие съёмных элементов конструкции. Легкосъёмные “штатные” элементы конструкции в обязательном порядке снимаются для осмотра внутренних полостей, имеющихся в подоконнике.

Внимательно осматривается “стык” подоконника со стеной, а так же “стык” рамы и оконного проёма, особое внимание нужно обратить на имеющиеся щели и полости.

Рамы осматриваются в открытом и в закрытом положении окон.

Особенности осмотра пластиковых окон.



Пластиковые окна “по определению” имеют особенности конструкции, позволяющие использовать их для внедрения средств съёма информации. Причём злоумышленнику не обязательно устанавливать какое-то “сложное” закладное устройство в профиль оконной рамы – достаточно использовать “штатные” пустоты подоконника, закрываемого с боков крышкой.

Пример идеальной “нычки”, находящейся в пластиковом подоконнике.

Снять торцевую крышку, установить в открывшуюся полость закладное устройство *(например, миниатюрный цифровой диктофон)* и поставить крышку на место – весь процесс займёт у злоумышленника меньше минуты.

Конструктивные полости в подоконнике обязательно внимательно осматриваются с использованием фонаря.

Очень полезен будет эндоскоп – если он есть.

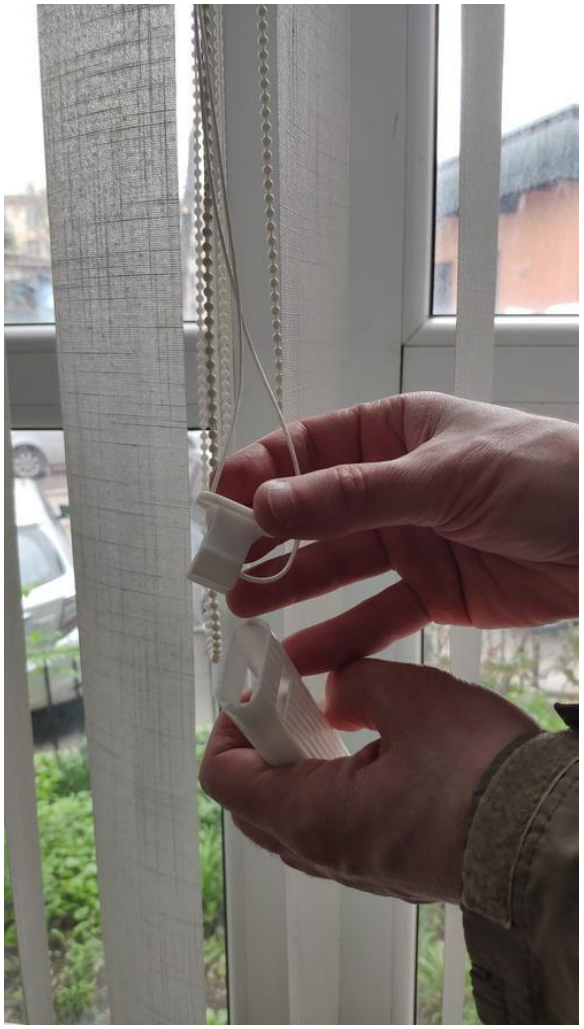
Осмотр оконных штор.

Внимательно осмотреть все занавески, шторы и жалюзи, а так же конструкции, на которых они крепятся.

Особое внимание обратить на внутренние поверхности и полости карнизов.

При осмотре штор *(особенно “массивных”)* внимательно проверить “складки”, а так же возможные “карманы” – обычно бывают в верхней и в нижней части шторы.

Пример “нычки”, находящейся в конструкции жалюзи.



Идеальная “нычка” находится в “противовесе” вертикальных жалюзи – *вообще такое впечатление, что этот “противовес” сделан специально для установки в него средств съёма информации*.

Данные элементы *(“противовесы”)* **обязательно открываются** и **осматриваются**.

Осмотр внешней стороны окон.

Внимательно осмотреть внешнюю часть оконной рамы и прилегающие к оконному проёму участки наружной стены, чтобы убедиться в отсутствии на них посторонних предметов непонятного назначения.

Осмотр внешней стороны окон – *примеры возможных устройств съёма информации*.

Пример радиостетоскопа и стетоскопа с передачей по ИК-каналу – *устройства подобного типа могут быть прикреплены на внешнюю часть оконной рамы или “околооконный” участок наружной стены.*

Осмотр батарей отопления.

Батареи отопления – *особенно если они закрыты декоративными крышками* – очень удобное место для установки устройств съёма информации.

При осмотре батарей обязательно потребуется фонарь и малое зеркало.

И **руки**, которыми нужно всё “прощупать”.

Осмотр батарей отопления.

<u>Обязательно</u> снять декоративные крышки *(решётки)*.

Осмотреть крышки и элементы их крепежа, при этом *особое внимание обратить на внутреннюю сторону*.

Внимательно осмотреть всё пространство за решётчатым ограждением.

Осмотреть и “прощупать” поверхность батарей – *особое внимание обратить на тыльную сторону и пространство между “рёбрами”*, пространство между батареей и стеной, а также места входа труб отопления в стены или пол *(потолок)*.

Осмотр пластиковых кабель-каналов *(коробов)*.

Современные кабель-каналы могут быть использованы для установки различных средств съёма информации: как устройств аудиоконтроля и видеонаблюдения, так и устройств контроля систем телекоммуникаций.

Необходимо снять крышки коробов и внимательно осмотреть кабель-каналы на наличие в них посторонних предметов.

При работе не забывать про **правила электробезопасности**!

Осмотр пластиковых кабель-каналов *(коробов)*.

Если полностью “открыть короба” не представляется возможным, то необходимо осмотреть кабель-каналы в наиболее вероятных *(“удобных” с точки зрения доступа злоумышленника)* местах возможной установки средств съёма информации.

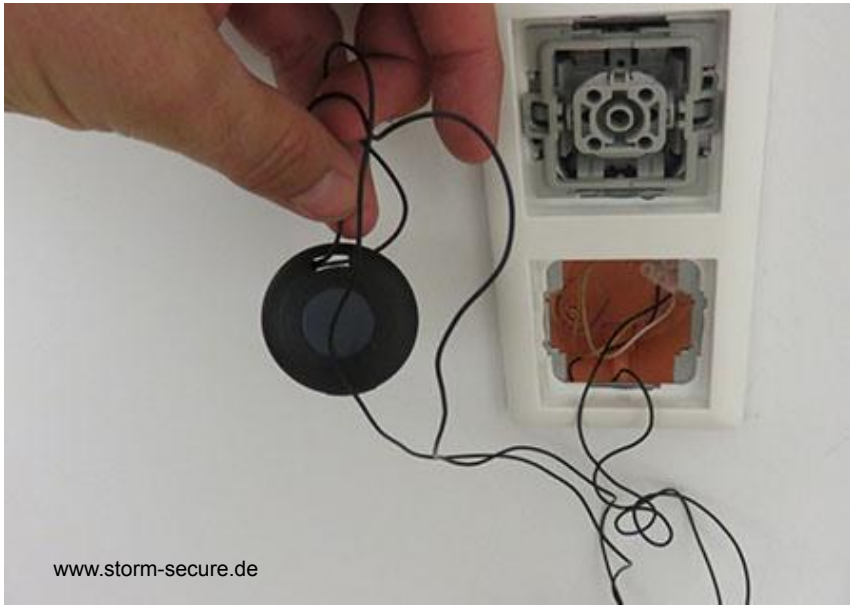
Если “ситуация с открытием коробов совсем сложная”, то можно использовать эндоскоп *(если он имеется в наличии)*.
Но всё-таки лучше стараться провести “живой” осмотр.

При работе не забывать про **правила электробезопасности**!

Осмотр пластиковых кабель-каналов *(коробов)*.

Учитывая, что в кабель-каналах прокладываются кабели различных систем –
как электропитание, так и “слаботочные” коммуникации –
при осмотре коробов нужно не только искать “заносные” устройства съёма информации, возможно установленные там, но и внимательно проверить элементы данных систем.
Если возникнут какие-либо “непонятные моменты”, то нужно проконсультироваться с электриком или с сотрудником подразделения IT, которые обслуживают данные системы.

Осмотр электророзеток и электровыключателей.



Электророзетки, выключатели, распределительные коробки *(“дозы”)* должны быть вскрыты и внимательно осмотрены.

При работе **соблюдать правила электробезопасности**!

В случае профессионального закладного устройства, выполненного “заводским” способом, обнаружить его в ходе визуального осмотра будет очень сложно *(иногда практически невозможно)* даже разобрав розетку – *в первую очередь это касается средств аудиоконтроля*.

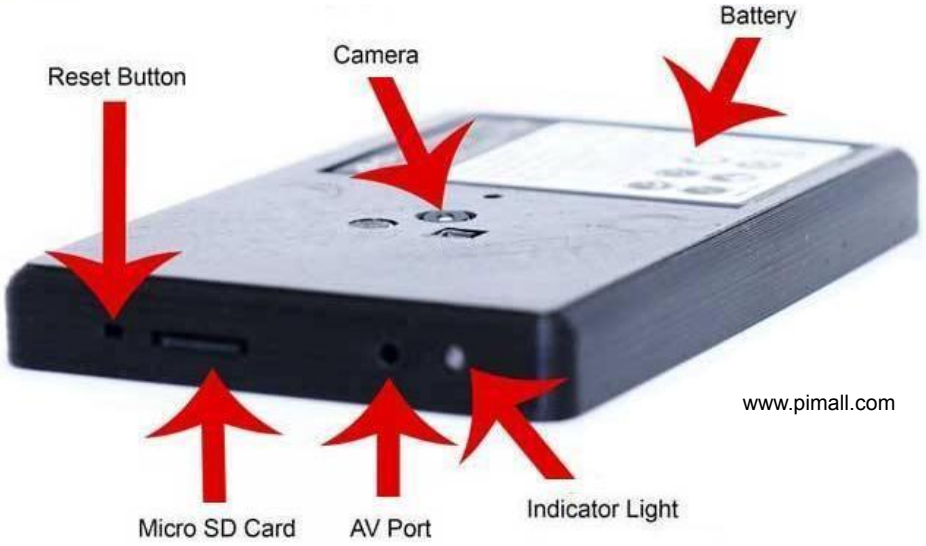
Осмотр электророзеток и электровыключателей.

В ряде случаев злоумышленник может использовать “фальшивые” электророзетки или электровыключатели, которые вообще не подключены к электросети, а являются автономными закладными устройствами.

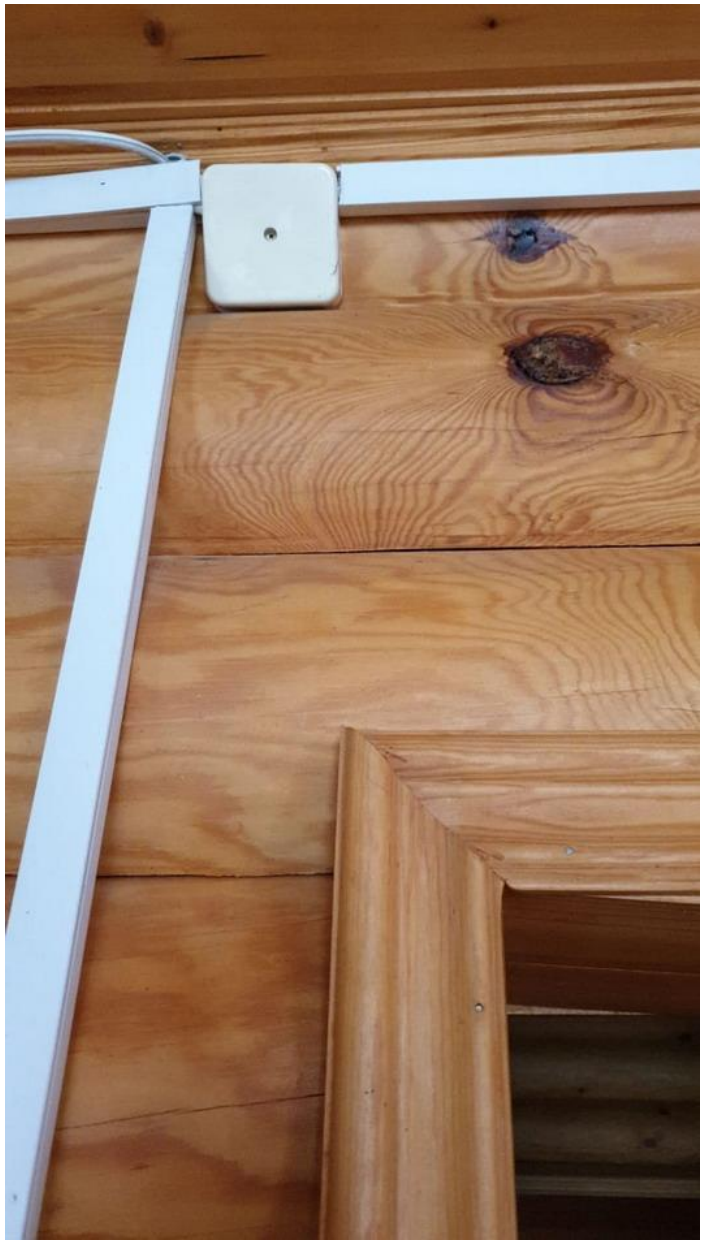
Как правило, такие “закладки” возможны на “чужой территории” – например, в гостиницах.

При внимательном осмотре такие закладные устройства легко обнаружить – при вскрытии “фальшивой” электророзетки или выключателя сразу будет видно, что это “закладка”.

Поэтому **вскрытие электророзеток и выключателей** при проведении осмотра помещения – **обязательно**.



Осмотр распределительных коробок *(“доз”)* – если к ним есть доступ.



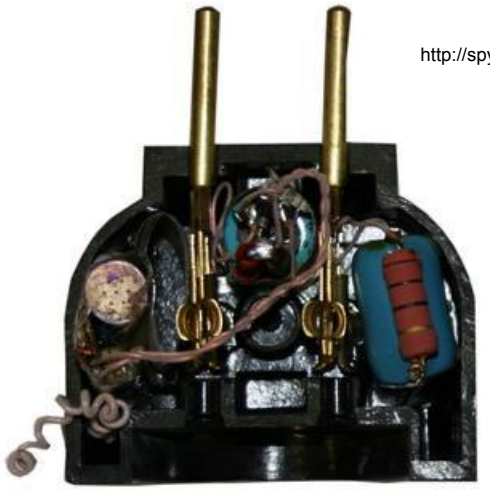
Электрические “дозы” открываются и внимательно осматриваются на предмет посторонних устройств, находящихся в них и подключённых к электросети.

При работе **соблюдать правила электробезопасности**!

Осмотр электроудлинителей, “тройников” и т.п.

При работе **соблюдать правила электробезопасности**!

http://spyby.net/articles/18-podslushivayuschie-ustroystva.html



Электроудлинители, “тройники” и т.п. <u>отключаются *(отсоединяются)*</u> от сети, разбираются и осматриваются.

*Как было сказано ранее, необходимо вести “**учёт**” и “**маркирование**” данных изделий – речь идёт о “своей территории”.*

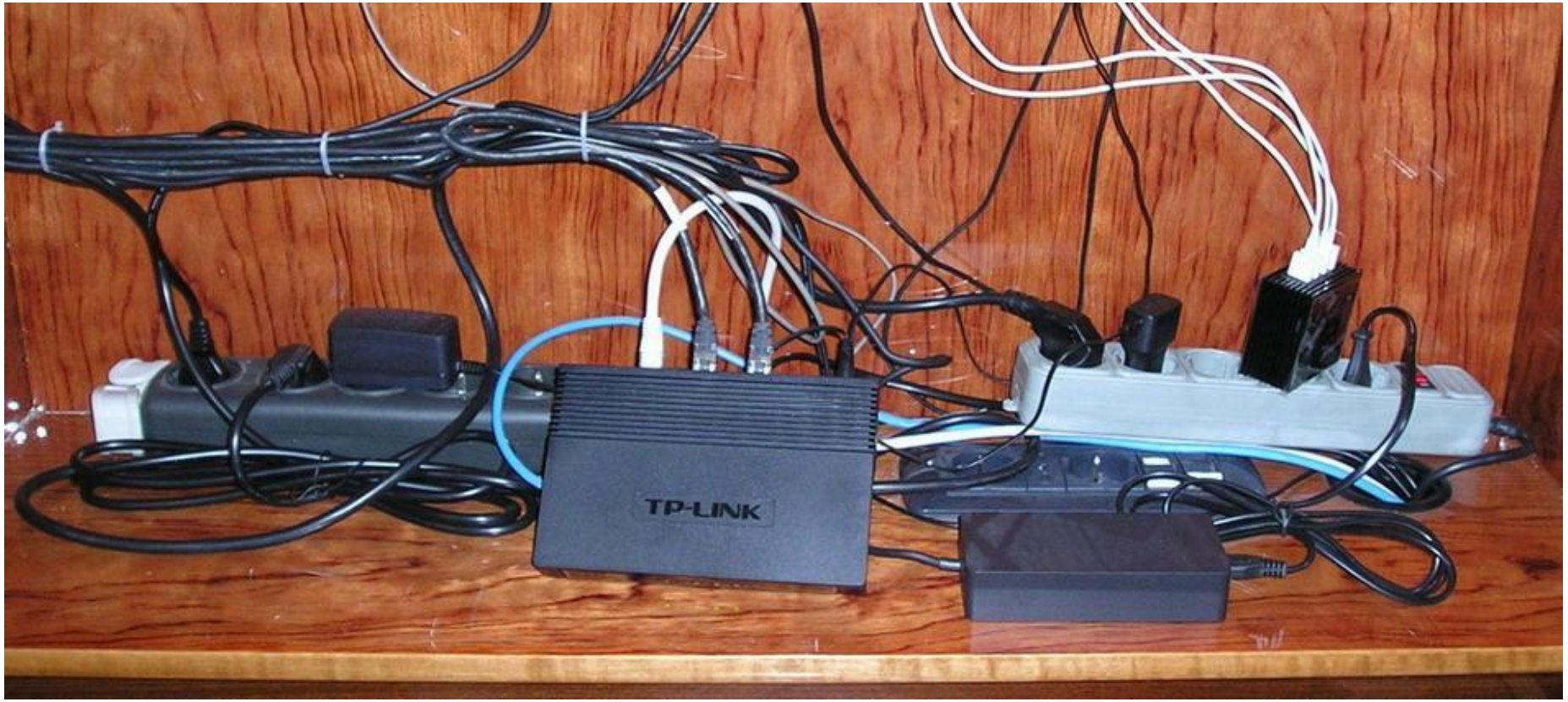
Осмотр “неразборных” электроудлинителей, “тройников” и т.п.

www.pimall.com

Некоторые электроудлинители, “тройники” и т.п. могут быть выполнены в *“неразборном” исполнении* и их физически нельзя разобрать *(без повреждения)* для внутреннего осмотра. В этом случае необходим особо тщательный внешний осмотр данных изделий – *с его помощью могут быть обнаружены возможно внедрённые видеокамеры*. Что касается “чисто акустических” устройств съёма информации, выполненных “заводским” способом, то их обнаружение в ходе внешнего визуального осмотра может быть весьма проблематично *(часто невозможно)*.

*Поэтому сразу после покупки данные изделия необходимо “**взять на учёт**” и “**промаркировать**”, а при осмотре сверить их серийные номера (скрытые метки), чтобы убедиться в отсутствии подмены.*

Осмотр зарядных устройств, блоков питания и т.п.



Зарядные устройства, блоки питания и т.п., находящиеся на “своей территории”, должны состоять на “учёте” и быть “промаркированы”.
При их осмотре необходимо сверить серийные номера *(скрытые “метки”)*, чтобы убедиться в отсутствии “подмены”.

Особенности осмотра зарядных устройств, блоков питания и т.п.

Осмотр зарядных устройств, блоков питания, электроудлинителей и т.п. является очень важным моментом, так как именно в них могут быть установлены различные устройства съёма информации, работающие как в режиме “накопителя”, так и в режиме “передатчика” – в том числе используя для передачи информации сотовую связь, Wi-Fi и Bluetooth *(очень актуально)*.

Если в блок питания или в зарядное устройство установлена видеокамера, то её можно будет обнаружить при тщательном визуальном осмотре, так как объектив камеры обязательно должен “иметь выход наружу”.

Совсем другая ситуация с обнаружением устройств аудиоконтроля: хорошо если для микрофона сделано отверстие в корпусе изделия – тогда при внимательном осмотре можно увидеть “накол” и сделать “соответствующие выводы”.
Но очень часто специального отверстия для микрофона не требуется – это значит, что нет никаких “внешних признаков” внедрения закладного устройства.

Особенности осмотра зарядных устройств, блоков питания и т.п.

Необходимо отметить, что практически все блоки питания для ноутбуков и другой электронной техники, а так же большинство зарядных устройств для мобильных телефонов и некоторые модели электроудлинителей выполнены в “литом” исполнении и не подлежат “разборке”. *Точнее, “разобрать” их конечно можно, а вот потом “собрать” и чтобы изделие ещё и нормально работало – это маловероятно*.

Поэтому основным правилом является “**учёт** и **контроль**”: сразу после покупки данные изделия необходимо взять “на учёт” *(“промаркировать”)*, а далее при проверках контролировать отсутствие “подмены”.

Особенности осмотра зарядных устройств, блоков питания и т.п.

Помнить про правило
“**Учёт и контроль**”.

Пример зарядного устройства,
которое можно разобрать для осмотра
(что бывает очень редко).

Как было сказано, в большинстве случаев
разборка блоков питания и
зарядных устройств
практически невозможна
без их повреждения, так–как они
выполнены в “литом” исполнении.

Но даже, если есть возможность
разобрать зарядное устройство,
далеко не всегда можно “легко”
определить наличие в нём “закладки” –
в первую очередь это касается
профессиональных радиомикрофонов,
установленных “заводским” способом.

Пример видеорекордера, камуфлированного в зарядном устройстве.

Отверстия под видеокамеру и микрофон, сделанные в корпусе зарядного устройства, могут быть обнаружены при внимательном внешнем осмотре.

Но нужно помнить, что в случае “чисто акустической закладки” специально сделанного отверстия в корпусе может и не быть. Поэтому основное правило: “**Учёт и контроль**”.

www.spyshop-online.com

Осмотр пола.

Конструкция пола в каждом конкретном помещении может быть различной *(паркет, ламинат, плитка, ковролин, линолеум и т.д.)*.

Если *не рассматривать угрозу “глубокого камуфляжа”*, то основные правила осмотра пола следующие: обязательно приподнять и осмотреть ковры и другие легкосъёмные напольные покрытия, а в случае “приклеенного” покрытия *(ковролин, линолеум)* внимательно осмотреть “стыки” со стенами *(плинтусами)*, различные “уплотнения”, места “вздутия”, надрезы, и т.п.

Если покрытие пола “собрано” из отдельных элементов: *плитка, паркет, ламинат и т.п.*, то нужно проверить надёжность крепления этих элементов и отсутствие явных следов их возможного вскрытия и последующей “заделки”.

Осмотр пола.

Если в полу предусмотрены подпольные каналы, то необходимо открыть съёмные крышки *(решётки)* и внимательно осмотреть открывшееся пространство на наличие в нём посторонних предметов и “непонятных” устройств.

Внимательно осмотреть места сквозного прохождения через пол труб отопления и коммуникационных стояков.

При наличие в помещении системы “тёплый пол” или системы вентиляции в полу, необходимо открыть съёмные крышки *(решётки)* и внимательно осмотреть открывшееся пространство.

Осмотр плинтусов.

Обычно встречаются два типа плинтусов: “цельные” *(как правило деревянные)* и “полые” *(как правило пластиковые)* – со встроенным кабель-каналом.

Полые плинтуса могут не только “прикрывать” средства съёма информации, но и быть местом их непосредственной установки.

Необходимо учитывать такой момент, как надёжность крепления плинтусов. Очень часто, когда начинаешь “разбирать” плинтус, он просто “разваливается” – в первую очередь это касается дешёвых пластиковых плинтусов.

Осмотр плинтусов.

Как правило, за плинтусами “прячут” элементы проводных микрофонов.

Нужно понимать, что для установки таких систем злоумышленник должен иметь возможность *“спокойно работать”* в нужном помещении достаточно длительное время.

В то же время, миниатюрные диктофоны или радиомикрофоны могут быть достаточно легко установлены внутри “полого” плинтуса или между стеной и плинтусом *(если он “болтается”)*.

Проверка вентиляционных отверстий *(шахт)*.

Вентиляционные отверстия могут быть использованы злоумышленниками для установки как средств аудиоконтроля, так и виденаблюдения.

Кроме того, в большинстве случаев обычное вентиляционное отверстие или вентиляционная шахта – это идеальный естественный канал утечки акустической *(речевой)* информации и из него можно услышать “**мно-о-о-ого** интересного”.

Об этом нужно постоянно помнить и даже если при осмотре вентиляционного отверстия в нём ничего не обнаружено, необходимо понять – куда ведёт этот вентиляционный канал или дымоход.

Проверка вентиляционных отверстий *(шахт)*.

Как правило, для осмотра вентиляционных отверстий необходимы все три “основных орудия производства”: лестница, отвёртка и фонарик.
Желательно иметь и “малое” досмотровое зеркало.

Для вариантов, когда надо заглянуть “в глубину” воздуховода, будет полезен эндоскоп *(если он имеется в наличии)*.

Осмотр потолков.

В зависимости от конструкции потолка “глубина” его осмотра будет различной. Если для “обычного” потолка будет достаточно убедиться в отсутствии на нём “посторонних предметов”, то для “рельефных” потолков и потолков, отделанных декоративными панелями или потолочными плинтусами, потребуется тщательный осмотр с использованием стремянки.

Осмотр подвесных потолков – это отдельный вопрос.

Примечание: *как было сказано ранее, варианты угроз, связанные с проведением “глубокого камуфляжа” (типа “штробления” и т.п.), не рассматриваются.*

Осмотр подвесных потолков.

Осмотр подвесных потолков.

Надпотолочное пространство – идеальное место для установки средств съёма информации. Причём, если для видеокамеры нужен “выход” в контролируемое помещение *(отверстие в потолке)*, то устройства аудиоконтроля могут просто “лежать” за подвесным потолком.

Понятно, что “невооружённым глазом” очень сложно *(практически невозможно)* обнаружить небольшое отверстие в потолочной панели – если стоишь внизу и очень не хочешь залазить на стремянку и “копаться в пыли”.

Осмотр подвесных потолков.

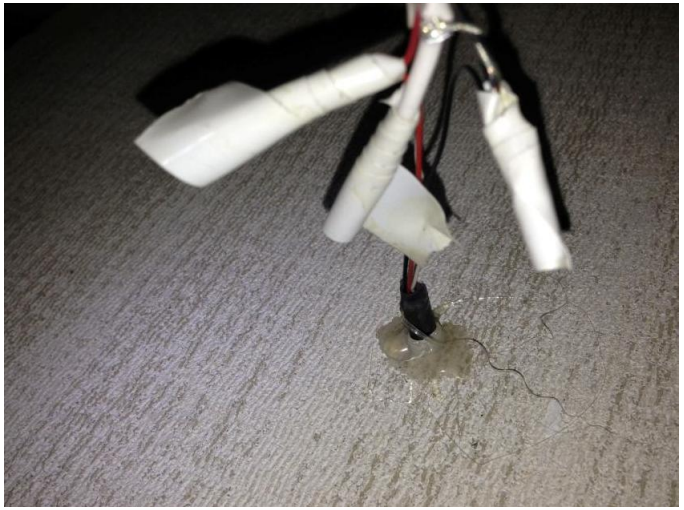
Тщательный осмотр надпотолочного пространства – обязателен.

При осмотре необходимо не только обращать внимание на “явно подозрительные” посторонние предметы, но и внимательно осмотреть *(разобрать)* все “штатные” элементы конструкции и коммуникаций, которых там много: “основной” потолок и стены, сами подвесные панели, элементы крепежа, датчики, распределительные коробки, свёрнутые в “бухту” кабели и т.д.

Для качественного осмотра нужно “сдвинуть” необходимое число подвесных панелей – чтобы получить доступ ко всей площади потолка.

При работе **не забывать про технику безопасности**!

Осмотр подвесных потолков.



Как правило, при “полноценном” доступе к надпотолочному пространству и внимательном осмотре, вероятность обнаружения возможных средств съёма информации будет высокой.

При отсутствии “полноценного” доступа, можно воспользоваться эндоскопом – *если он имеется в наличии* – но <u>всё же желателен именно “живой” осмотр</u>.

Осмотр подвесных потолков с использованием эндоскопа.

Осмотр подвесных потолков с использованием телевизионной досмотровой системы.

www.reiusa.net

Даже если есть возможность использовать эндоскоп или телевизионные досмотровые системы, то необходимо помнить, что они дают только “общую картину” – имеется ввиду, что <u>все подозрительные места</u> *(которых за подвесным потолком очень много)* в любом случае <u>надо “осмотреть вживую” и “пощупать руками”</u>.

Одно дело использовать такие системы для осмотра “ровных” поверхностей, на которых не должно быть ничего, и другое дело осматривать подвесной потолок – где “сплошные рёбра” и много “всякой всячины”.

Осмотр датчиков ОПС, проводимый одновременно с осмотром потолка.

В ходе проведения осмотра потолка необходимо проверить и установленные на нём датчики охранно-пожарной сигнализации.

Как правило, устройства съёма информации, устанавливаемые в датчиках ОПС, выполнены в виде *“отдельного модуля непонятного назначения”* и их легко обнаружить при вскрытии датчика.

Но тут **есть один момент**, который необходимо помнить при разборке датчика: в большинстве систем ОПС предусмотрена “аварийная сигнализация на вскрытие датчиков” и соответствующий сигнал уйдёт на пульт охраны – *даже если объект “снят с сигнализации”*.

Поэтому такой осмотр желательно совместить с проведением технического обслуживания системы ОПС или предупредить оператора, что датчики будут вскрываться – если нет возражений.

Осмотр датчиков ОПС, проводимый одновременно с осмотром потолка.

www.pimall.com

При осмотре датчиков ОПС необходимо обращать внимание как на различные отверстия в корпусе – *за ними могут размещаться камера или микрофон*, так и *на наличие слотов под SIM-карту или карту памяти*.

При наличии в датчике SIM-карты или карты памяти нужно разбираться – это “штатная” карта, которая предусмотрена для работы системы сигнализации, или это карта от установленного в датчик закладного устройства.

Осмотр потолочного освещения *(общие моменты)*.

В зависимости от объекта, потолочное освещение может быть самым разным: *от простой “трёхрожковой” люстры, которая есть в обычной квартире, до сложной “системы иллюминации”, состоящей из целого набора “висячих” хрустальных люстр и “встроенной” подсветки*.

При осмотре потолочного освещения **обязательно понадобится стремянка** и **досмотровые зеркала**.

В ходе осмотра **основное внимание необходимо обратить** на наличие “посторонних предметов”, находящихся в конструктивных полостях, прикреплённых к элементам люстр, подключённых к проводам и т.д.

Учитывая, что произвести “полную разборку” устройств электроосвещения сможет не каждый, то без наличия нужной подготовки этого делать не надо – *при необходимости нужно привлекать штатного электрика*.

При работе соблюдать **правила электробезопасности**!

Осмотр потолочного освещения – *пример типовой “висячей” люстры*.

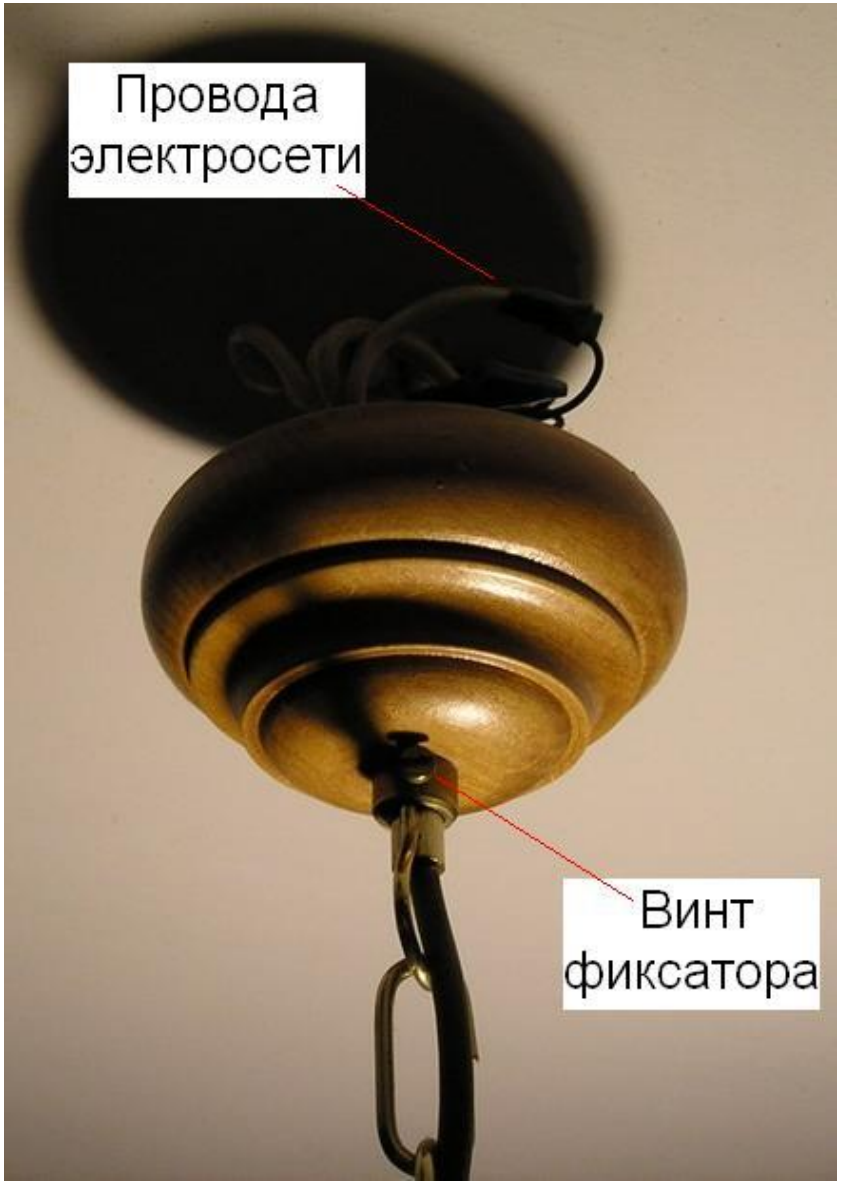
В любой люстре найдётся место для диктофона или радиомикрофона – вопрос в том, как туда “добраться” злоумышленнику для их установки.

В большинстве “висячих” люстр имеются две “типовые точки” (***см. фото***), которые могут быть использованы злоумышленником для установки средств съёма информации.

Понятно, что в люстре имеется гораздо больше “слабых” мест – *например, “закладка” может быть внедрена непосредственно внутрь корпуса люстры* – но сейчас речь идёт о тех случаях, когда злоумышленник имеет только кратковременный доступ к уже “висящей” люстре и не может её разбирать или снимать с потолка.

“Скрытая” полость *(“стакан”)* и “открытая” полость *(“чаша”)* **обязательно** осматриваются.

Осмотр потолочного освещения – *пример типовой “висячей” люстры*.



В большинстве “висячих” люстр имеется “**скрытая**” полость, закрываемая крышкой, в которой “спрятаны” провода электросети – *так называемый “стакан”*.
При удачном “раскладе” – *доступ “наверх” и около 10 минут “спокойной” работы* – злоумышленник может установить там радиомикрофон, который будет “запитан” от электросети – *правда, работать такая “долговременная радиозакладка” будет только тогда, когда люстра включена*.

Осмотр потолочного освещения – *пример типовой “висячей” люстры*.

В большинстве “висячих” люстр имеется и “**открытая**” полость – как правило, имеющая форму *“чаши”* или *“блюдца”*.

В отличие от “скрытой” полости, речь о которой шла ранее, для установка “закладки” в “открытую” полость потребуется меньше минуты – злоумышленнику нужно только “дотянуться” до неё *(например, встав на стул)* и просто положить туда изделие, которое снизу никто не увидит.

<u>Типовой пример</u>: если у злоумышленника нет необходимости в получении информации в масштабе реального времени, то он может просто положить в “открытую” полость цифровой диктофон с заданными настройками – VOX, таймера и т.д. – который будет вести запись в течении недели или дольше. А при удобном случае диктофон будет изыматься для “скачивания” информации.

Осмотр потолочного освещения – *так называемые “умные лампы”* .

При проведении осмотра потолочного освещения необходимо обращать внимание не только на возможные *“посторонние предметы”*, но и помнить о том, что средства съёма информации могут быть встроены непосредственно в электролампочку. Как было сказано ранее, такие устройства часто выполнены на базе т.н. *“умных ламп”*, которыми можно управлять дистанционно по Wi-Fi: лампа выполняет свою “штатную” функцию *(свет)*, а кроме того имеет в своём составе встроенные камеру и микрофон.

Осмотр мебели.

Каждое помещение имеет свои особенности, в плане установленной в нём мебели: где-то вообще “голые стены”, где-то мебели немного и она “мобильна”, а где-то мебели очень много и она “встроена”.

Кроме того, различные типы мебели требуют “своего осмотра”: одно дело “голая поверхность” *(пусть и большая по площади)* и другое дело – диван или стол со множеством полостей, щелей и различных “*нычек*”.

При осмотре мебели есть основные правила, которые позволяют обнаружить большинство “заносных” средств съёма информации *(как было сказано раньше – о “глубоком камуфляже” речь не идёт)*.

Главный момент: должен быть обеспечен доступ ко всем поверхностям мебели – *в том числе и “внутренним полостям”* – это значит, что **мебель должна быть полностью освобождена от содержимого** и в ходе осмотра она должна “двигаться” и “переворачиваться”.

Осмотр мебели *(основные общие моменты)*.

Мебель отодвигается от стен (*если это возможно*) и друг от друга, чтобы обеспечить доступ ко всем поверхностям мебели.

Если отодвинуть мебель от стены не представляется возможным, то с помощью фонаря и зеркал (эндоскопа) осматривается пространство между мебелью и стеной.

Вынимается всё содержимое шкафов, столов, диванов и т.д.

Выдвижные ящики, полки и другие легкосъёмные элементы вынимаются и осматриваются.

Осматриваются **все поверхности мебели** *(верх, низ, боковые поверхности)*, а также пол *(напольное покрытие)* под отодвинутой мебелью.

Внимательно осматриваются и “прощупываются” все полости столов, диванов, кресел и.д. Для осмотра “скрытых” полостей полезен эндоскоп (если он есть).

При осмотре мягкой мебели осматриваются и “прощупываются” все её элементы, особое внимание обращается на соединительные швы и складки обивки.

В ходе осмотра мебели фактически параллельно решаются две задачи: осматривается сама мебель и осматривается содержимое, находящееся внутри или на мебели.

Примечание: *при осмотре мебели и её содержимого целесообразно работать в тонких матерчатых перчатках – в первую очередь это нужно, чтобы “не залапать” глянцевые и стеклянные поверхности – естественно, что это должны быть не те перчатки, в которых проводился осмотр подвесных потолков, вентиляционных шахт, полов и т.п.*

Некоторые “нюансы”, касающиеся осмотра мебели *(и не только мебели)*.

Для проверки различных щелей и пустот,
всегда присутствующих в элементах мебели,
очень полезными могут быть “щупы”,
в качестве которых можно использовать
обычные вязальные спицы
(пластмассовые или стальные).

Некоторые “нюансы” осмотра мебели в случае, когда её элементы нельзя отодвинуть от стены *(пола)* или друг от друга.

Если мебель “нетранспортабельна” и в ходе проведения проверки её нельзя отодвинуть или приподнять, то нужно обратить **особое внимание** на щели (“стыки”) между мебелью и стеной (полом), а так же между элементами мебели.

Необходимо помнить, что существуют устройства съёма информации, имеющие плоский корпус, которые могут быть установлены даже в узкую щель. Кроме того, нужно помнить о “бросовых” радиомикрофонах, которые могут быть установлены “на неизвлекаемость” – т.е. злоумышленник разово “забросил” их на объект (например, за шкаф) и в принципе не собирается оттуда забирать – изделие работает, пока у него не закончится электропитание и оно не “умрёт”.

Примеры “плоских” радиомикрофонов и диктофонов, которые могут быть внедрены в “щели” между элементами мебели.

www.endoacustica.com

Time of continuous operation	Dimensions(mm)
12 days	140 x 100 x 7
12 days	200 x 150 x 4
24 days	200 x 210 x 4
36 days	290 x 210 x 4

www.spyshop-online.com

www.telesys.ru

Некоторые “нюансы” осмотра мебели в случае, когда её нельзя приподнять от пола.

С помощью “щупа” тщательно проверяются щели между днищем “нетранспортабельной” мебели *(которую нельзя приподнять)* и полом.

Некоторые “нюансы” осмотра мебели в случае, когда её элементы нельзя отодвинуть друг от друга.

С помощью фонаря внимательно осматриваются все щели между элементами мебели. При необходимости нужно использовать “щуп”.

Некоторые “нюансы” осмотра мебели в случае, когда её элементы нельзя отодвинуть от стены или друг от друга.

Если в наличии имеется эндоскоп, то его нужно использовать для осмотра щелей (стыков) между мебелью и стеной (полом), а так же между элементами мебели.

Осмотр мебели *(рабочий стол)*.

Осматриваются **все** конструктивные поверхности стола.
Особое внимание обратить на различные конструктивные полости и пустоты *(в том числе в крышке и в днище стола)*.

Вынимается и **осматривается всё содержимое** стола. **Все выдвижные ящики** и **другие легкосъёмные элементы конструкции** так же вынимаются и осматриваются.

Некоторые “нюансы” осмотра мебели, в которой есть легкосъёмные элементы конструкции *(в том числе “выдвижные” ящики)*.

Необходимо помнить, что есть ряд “нюансов”, связанных с креплением легкосъёмных элементов мебели.

В частности, это касается выдвижных ящиков стола, которые “ездят” по специальным “направляющим”.

Поэтому вначале имеет смысл разобраться в конструкции крепления и “потренироваться” в съёме ящиков и **особенно** в установке на прежнее место, так как могут возникнуть определённые проблемы технического плана.

Данная ситуация характерна и для других легкосъёмных (если знать, как их снимать) элементов конструкции мебели, которые крепятся не на болтах и шурупах, а с помощью различного рода “клипс”, “защёлок”, специально сделанных пазов и т.п.

Вариант “Т-образного” рабочего стола.

Дополнительно обратить внимание на место “стыка” стола руководителя и примыкающего к нему стола для посетителей. Кроме того, обратить внимание на ножки стола для посетителей – очень часто они сделаны “полыми”.

Осмотр рабочего стола *(предметы на столе)*.

Внимательно осматриваются **все предметы**, находящиеся на столе.

При наличии портативного металлодетектора будет очень полезно проверить с его помощью деревянные и кожаные изделия: подставки, “стаканы”, папки и т.п.

*Если в компании **случайно** имеется рентгенотелевизионная установка – например, по линии антитеррора – то все “подозрительные” изделия на проверку.*

Осмотр рабочего стола *(содержимое ящиков)*.

Ящики стола вынимаются и внимательно осматривается их содержимое.

Бывают случаи, когда в отдельные ящики своего стола хозяин кабинета вообще не заглядывает и даже не знает, что в них лежит. Очень часто там “чего только нет” – и среди этого “барахла” могут находиться устройства съёма информации, в том числе камуфлированные (например, под “канцтовары”).

Осмотр канцелярских принадлежностей *(ручки, маркеры и т.п.)*.

Внимательно осматриваются все авторучки, фломастеры, карандаши и т.п.
Если это возможно, то производится их “разборка”.

При “разборке” дорогих изделий – например, авторучек с золотым пером за 1500 – 2000 USD, нужно быть очень аккуратными, чтобы случайно их не сломать. Если не понятно, как такое изделие разбирается, то лучше “не экспериментировать” .

Осмотр канцелярских принадлежностей *(ручки, маркеры и т.п.)*.

При наличии портативного металлодетектора будет очень полезно проверить с его помощью все канцелярские изделия, не содержащие металлических элементов: маркеры и авторучки в пластиковых корпусах, “клеящие” карандаши и т.д.

*Если в компании **случайно** имеется рентгенотелевизионная установка (например, по линии антитеррора), то всю эту “канцелярскую мелочёвку”, которую нельзя разобрать, нужно отправить туда на проверку.*

Осмотр мебели *(кресла и стулья)*.

С точки зрения злоумышленника кресла и стулья “интересны” тем, что они находятся рядом с *“источником звука”* – на них сидят люди, ведущие разговор. Кроме того, кресла и стулья могут иметь много “удобных” мест для установки средств съёма информации.

При проверке стульев внимательно осматриваются и “прощупываются” как все “открытые” поверхности – *особое внимание обратить на днища*, так и все возможные полости, щели, соединительные швы и т.д. Производится разборка *(съём)* всех легко отсоединяемых элементов конструкции.

Осмотр мебели *(кресла)*.

Снимается “**всё, что можно снять**” и осмотреть отдельно: подушки, “пуфики”, покрывала и т.д. Внимательно осматриваются и “прощупываются” как все “открытые” поверхности – ***особое внимание*** *обратить на днище*, так и все возможные полости, щели, соединительные швы, складки обивки и т.п.

Осмотр мебели *(диваны и другие элементы комнаты отдыха)*.

Комната отдыха очень часто используется для переговоров, проводимых “с глазу на глаз”. Её типовое “оснащение”: диван, пара кресел, журнальный столик, тумба с цветами.

Осмотр дивана начинается с его “разборки” – снимается “**всё, что можно снять**” и осмотреть отдельно: подушки, “пуфики”, покрывала, вынимается всё внутреннее содержимое, а так же отсоединяются легкосъёмные элементы конструкции. Внимательно осматриваются и “прощупываются” как все “открытые” поверхности – ***особое внимание*** *обратить на днище*, так и все возможные полости, щели, соединительные швы, складки обивки и т.п.

Журнальные столики, кресла, тумбы и т.д. осматриваются по аналогии с тем, как было изложено выше.

Осмотр мебели *(диван)*.

Диван имеет множество мест, куда могут быть установлены средства съёма информации – по числу возможных “нычек” это один из “лидеров” среди мебели *(моё личное мнение)*.

Осмотр мебели *(шкаф)*.

Шкафы бывают разной конструкции и назначения.

При осмотре шкафа необходимо вынуть и осмотреть **всё** его **содержимое**.

Выдвижные ящики, полки и другие легкосъёмные элементы вынимаются и осматриваются.

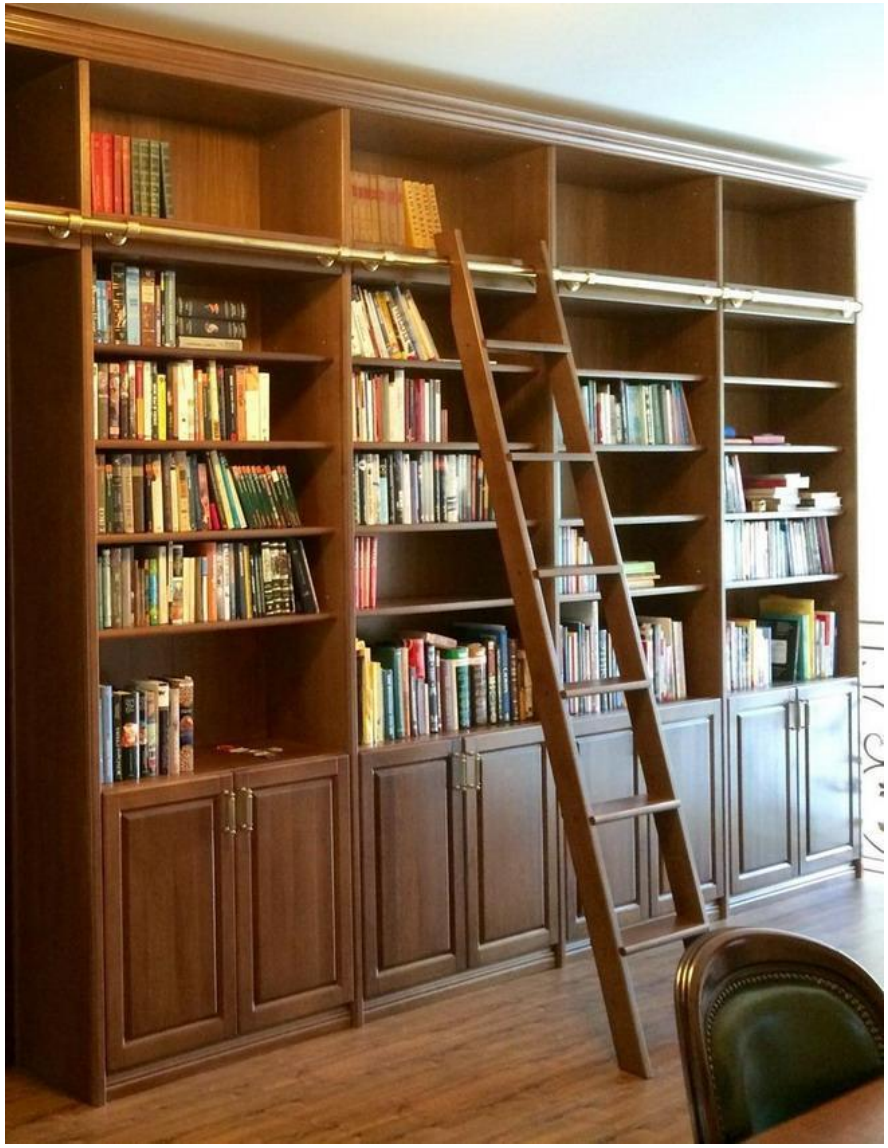
Осматриваются все конструктивные поверхности шкафа.

Особое внимание обратить на различные конструктивные полости и щели: *в днище, в местах стыка элементов конструкции, для встроенной подсветки и т.д*.

Если шкаф нельзя отодвинуть от стены, то внимательно осмотреть “стык” шкафа и стены.

Пример осмотра содержимого, находящегося в шкафу:
каждый объект аккуратно вынимается и осматривается (осмотр предметов интерьера далее будет рассмотрен более подробно).

Осмотр книжных шкафов.



Книжный шкаф или даже “библиотека”, как правило, обязательно присутствует на большинстве объектов: будь то работа, дом или “чужая территория”.

Кто-то держит книги “для красоты” *(точнее сказать “для солидности”)*, живя по принципу: *“понты дороже денег”*.

Кто-то рассматривает книги как элемент “коллекционирования” – как у Портоса в “Виконте де Бражелоне”: *“Моей библиотеки, насчитывающей шесть тысяч совершенно новых и никогда не раскрытых томов”*.

Кто-то – *хотя таких, к сожалению, всё меньше и меньше* – любит читать и каждая книга, стоящая на его полке, прочитана и перечитана несколько раз.

Кроме того, книжный шкаф – типовой “атрибут” конференц-залов, гостиниц и т.п.

Осмотр книжных шкафов.

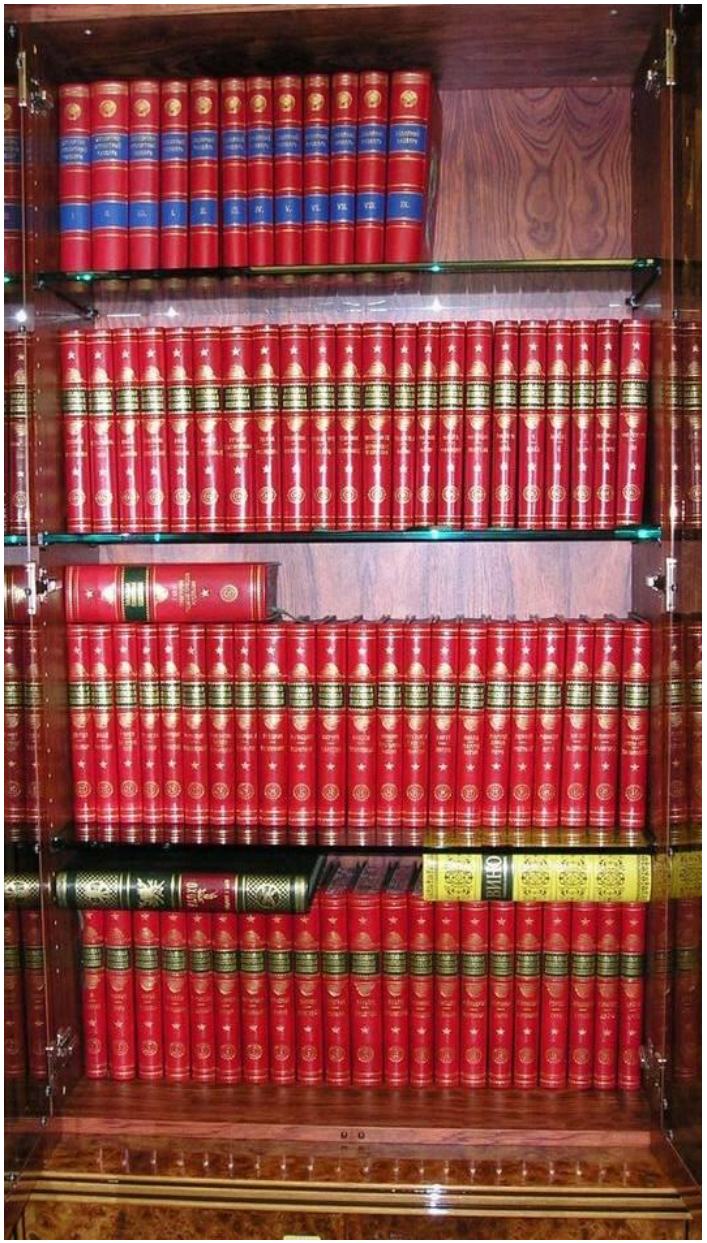
С точки зрения поиска устройств съёма информации книжный шкаф является сложным объектом, который требует тщательного и длительного осмотра.

Это связано с тем, что данные устройства могут быть внедрены как в конструкцию самого шкафа *(особенно, если шкаф имеет скрытые полости)*, так и находиться “просто среди книг” или внутри их.

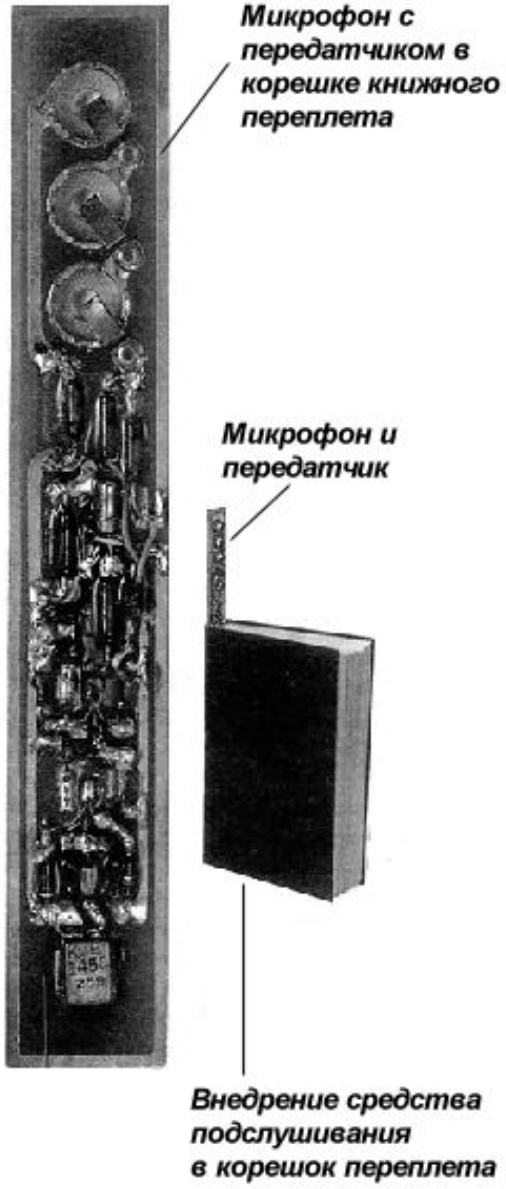
Причём совсем не обязательно, чтобы злоумышленник использовал какие-то сложные устройства с “глубоким камуфляжем”, которые “вживляются” в книгу – достаточно типового “GSM-передатчика” размером со спичечный коробок, который “лежит” за книгами.

С миниатюрными цифровыми диктофонами ещё проще: заданы “таймера”, включён “VOX” и диктофон может работать неделю и более.

А если диктофон “плоский” – *например, в виде банковской карты* – то он может быть легко установлен даже между страниц любой книги.



Осмотр книжных шкафов.



В качестве “классического” примера подслушивающих устройств, которые появились ещё после второй мировой войны, можно привести выдержку из статьи “**Кит Мэлтон и его музей “шпионской техники”**” *(В.А.Шелков, “Специальная техника” № 1-2, 1999 г.)*:

“Другое хитроумное устройство легко умещалось в корешке переплёта обыкновенной книги средней толщины. Такую книгу можно было без особых подозрений поставить на полку в интересующем разведку помещении. Приведённые здесь примеры характерны для 60-х годов. В наши дни, благодаря использованию современной технологии, средства подслушивания стали еще более миниатюрными”.

www.gcomtech.com

“Кит Мэлтон и его музей “шпионской техники””, В.А.Шелков, “Специальная техника” № 1-2, 1999 г.

Осмотр книжных шкафов.

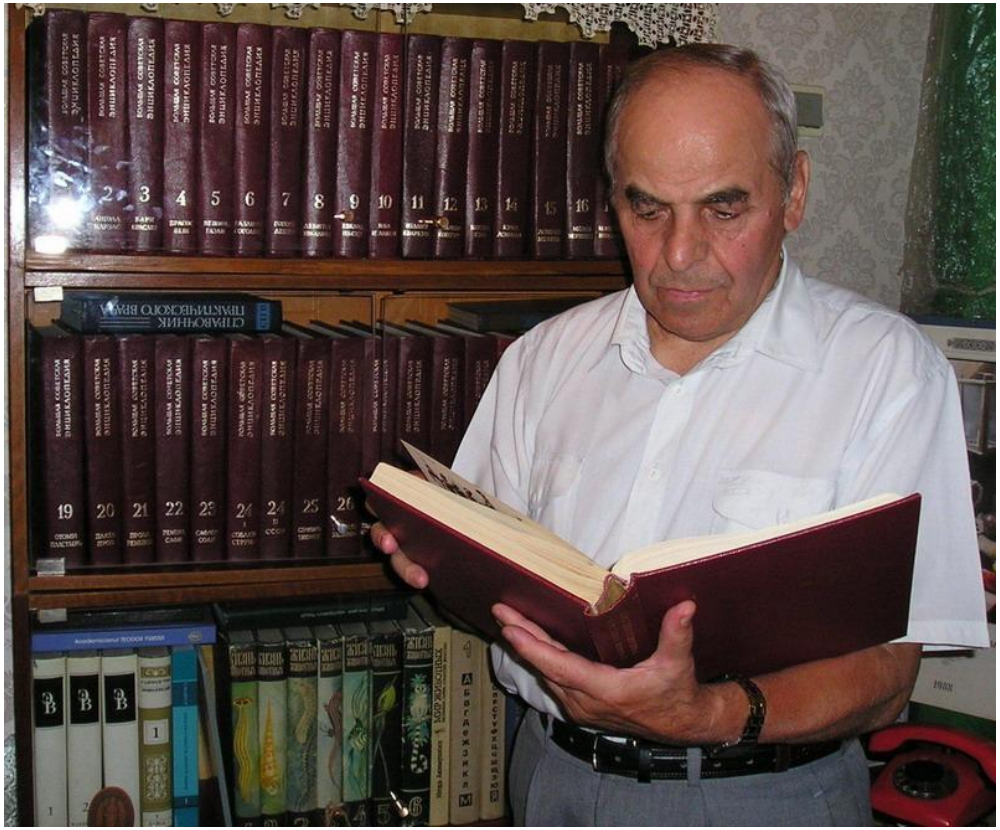
В книгу, “лежащую на полке”, может быть установлено и устройство видеозаписи. Причём не обязательно с “камуфляжем” – например, видеорекодер, который “просто положен” между страницами книги и “направлен в нужную сторону”.

www.pimall.com

Осмотр книжных шкафов.

При проведении “**полного осмотра**” книжного шкафа необходимо освободить полки и осмотреть шкаф, обращая особое внимание на его конструктивные полости и щели.

Каждая книга осматривается и *“пролистывается”*, при этом **особое внимание** обращается на корешок переплёта и на “суперобложку” *(если она есть)*.



При наличии портативного металлодетектора будет очень полезно проверить с его помощью те книги, в которые могут быть “глубоко” внедрены закладные устройства: например, книги с толстой жёсткой обложкой.

*Если в компании **случайно** имеется рентгенотелевизионная установка – например, по линии антитеррора – то все “подозрительные” книги на проверку.*

Осмотр книжных шкафов *(полок)*.

Естественно, что “полный осмотр” даже обычного книжного шкафа – *а тем более библиотеки* – это очень трудоёмкий процесс и его не получится проводить “ежедневно” или по команде *“срочно за десять минут”*.

Поэтому **очень важно** чётко представлять все возможные угрозы и выработать оптимальную периодичность и “глубину” проверок для каждого конкретного объекта.

Ну а по жизни нужно помнить классическую фразу: “**Книга – источник знаний**”.

И **читать книги** – **хорошие**, **естественно**.

Осмотр “канцелярских” шкафов *(канцелярские папки)*.

Канцелярские папки, стоящие на полках, являются очень удобным местом для установки устройств съёма информации – *в частности, видеокамер и диктофонов*.

Осмотр “канцелярских” шкафов *(канцелярские папки)*.

Каждая папка внимательно осматривается – при этом “пролистываются” и “прощупываются” все подшитые в ней “файлы” с документами.

Осмотр отдельных предметов интерьера *(общие моменты)*.

В помещении могут находиться самые разнообразные предметы интерьера, поэтому в каждом конкретном случае нужно исходить из реальной ситуации: что-то может быть проверено простым внешним осмотром, где-то потребуются фонарик и “щуп”, а в ряде случаев будет необходимо разобрать предмет.

Основное правило: *каждый предмет должен быть внимательно осмотрен и, по возможности, разобран*.

При осмотре предметов интерьера нужно “оценивать” возможность использования конкретного предмета для внедрения в него средств съёма информации. Надо чётко понимать, что закладное устройство может быть не только просто “прикреплено” к какому-либо предмету или “лежать” в нём *(например, в вазе)*, но и быть“глубоко закамуфлировано” в этот предмет – *в том числе , “заводским” способом*.

Для предметов интерьера очень актуальным является правило “**Учёт и контроль**”: сразу после приобретения предмет должен быть проверен и его нужно взять “на учёт” и “промаркировать”, а в ходе дальнейших проверок контролировать отсутствие “подмены”. Как уже было сказано, очень часто этого не делают, т.к. не хотят “заморачиваться”. А зря…

Далее приведены несколько примеров осмотра некоторых “типовых” предметов интерьера.

Осмотр предметов интерьера *(статуэтки, вазы, пепельницы и т.п.)*.

Предметы тщательно осматриваются, при этом **особое внимание** обращается на различные полости, подозрительные отверстия и щели, а так же на наличие элементов, не характерных для предметов данного типа: *слотов под SIM-карту или карту памяти*, *каких-либо встроенных разъёмов (мини-USB или типа для “зарядки”) и т.п*.
Все съёмные элементы аккуратно отсоединяются для тщательного осмотра.

При наличии портативного металлодетектора будет очень полезно проверить с его помощью все неметаллические изделия.

*Если в компании **случайно** имеется рентгенотелевизионная установка – например, по линии антитеррора – то все “подозрительные” изделия на проверку.*

Осмотр предметов интерьера *(статуэтки, вазы, пепельницы и т.п.)*.

Пример осмотра предметов интерьера *(вазы)*.

Вазы осматриваются внутри и снаружи, при этом ***особое внимание*** *нужно обратить на внутреннюю полость и на днище – в нём тоже может быть конструктивная полость (“выемка”)*.

При осмотре нужно быть очень аккуратным, чтобы не повредить изделие – *некоторые вазы могут быть достаточно хрупкими и могут треснуть просто при взятии их в руки*.

А если сломать вазу за десятку или пятнашку евро, то сами понимаете – в лучшем случае, придётся продавать квартиру…

Так что при осмотре хрупких изделий *(да и вообще при работе)* нужно быть очень внимательным.

Пример осмотра предметов интерьера – *скрытая видеокамера, установленная в декоративной вазе (освежителе воздуха).*

При внешнем осмотре видно отверстие для видеокамеры.
При осмотре внутренней полости можно найти закладное устройство, установленное в вазе.

Пример осмотра предметов интерьера – *пепельница, в которой установлен GSM-передатчик*.

Достаточно высокий уровень камуфляжа – GSM-передатчик установлен внутри корпуса и для доступа к нему необходимо снять крышку *(днище)*, открутив четыре винта.

В ряде случаев “шляпки” винтов могут быть скрыты наклейкой и на первый взгляд предмет может выглядеть как “неразборный” – *это надо иметь ввиду*.

Пример осмотра предметов интерьера *(настольная лампа)*.

Перед осмотром **необходимо** отключить *(отсоединить)* лампу от электросети.

Если это возможно, то корпус настольной лампы разбирается и внимательно осматриваются все внутренние полости.

В случае, если настольная лампа имеет “литой” неразборный корпус, то основным правилом является “**Учёт и контроль**”: сразу после покупки данное изделие нужно взять “на учёт” (“промаркировать”) и в ходе дальнейших проверок контролировать отсутствие “подмены”.

Осмотр предметов интерьера *(часы – общие моменты)*.

Часы имеются в большинстве как “рабочих”, так и “личных” помещений: в рабочем кабинете, переговорной комнате, зале совещаний, комнате отдыха, спальне и т.д.

В ряде случаев часы не просто “показывают время”, а являются *“необходимым элементом интерьера”* или *“предметом коллекционирования”*.

Очень часто часы поступают в качестве подарка, который устанавливают на “видное место”.

Часы могут иметь различную конструкцию и внешний вид, при этом с точки зрения злоумышленника они являются предметом, очень удобным для внедрения средств съёма информации: **во-первых**, часы обычно находятся в “нужных” местах, из которых удобно осуществлять аудио- и видеоконтроль за “интересующим объектом”, **во-вторых**, конструкция большинства часов позволяет использовать их как для быстрой установки “заносных” устройств съёма информации, так и для “глубокого камуфляжа” в них закладных устройств *(очень часто выполненных “заводским” способом)*.

Нужно понимать, что при визуальном осмотре часов можно обнаружить прикреплённые к ним “посторонние предметы” и некоторые варианты “глубокого камуфляжа” – *например, отверстие для видеокамеры*, но в случае *“заводского глубокого камуфляжа”* устройств аудиоконтроля – обнаружить закладное устройство без разборки часов практически невозможно.

Осмотр предметов интерьера *(механические часы с “боем”)*.

Часы внимательно осматриваются как снаружи – *особенно тыльная сторона и днище*, так и изнутри – ***особое внимание*** *обратить на различные внутренние полости*: это типовые места для установки средств съёма информации.

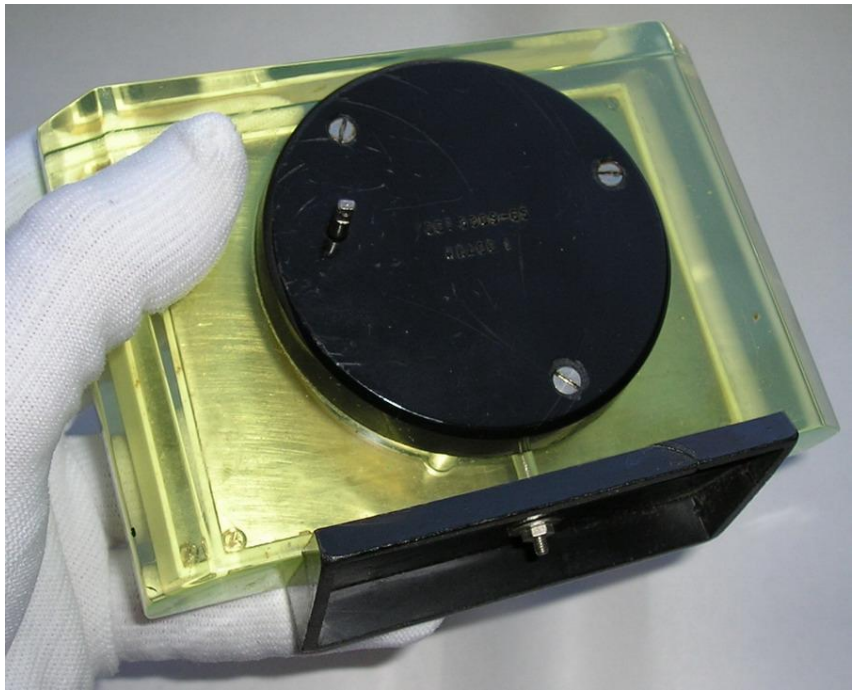
Как правило, такие часы выполнены в массивном корпусе (*деревянном или металлическом*) и “неподвижны” – т.е. для проведения с ними каких-либо ежедневных работ (*например, завода*) не требуется их перемещение или “переворачивание”, а достаточно просто “перетянуть” гири на часах или вставить ключ и завести часы. Поэтому владелец часов может длительное время не замечать, что “скрывается” *внутри*, *за* и *под* часами.

Осмотр предметов интерьера *(механические часы)*.

Часы внимательно осматриваются снаружи на предмет прикреплённых к ним посторонних предметов – *особенно тыльная сторона и днище.* ***Особое внимание*** *нужно обратить на различные полости – например, в подставке*.

В отличие от массивных часов с “боем”, о которых речь шла ранее, небольшие механические часы практически ежедневно “контролируются” хозяином, так как он их берёт в руки, чтобы завести. Поэтому при “заводе” посторонние предметы, прикреплённые к часам, будут обнаружены.

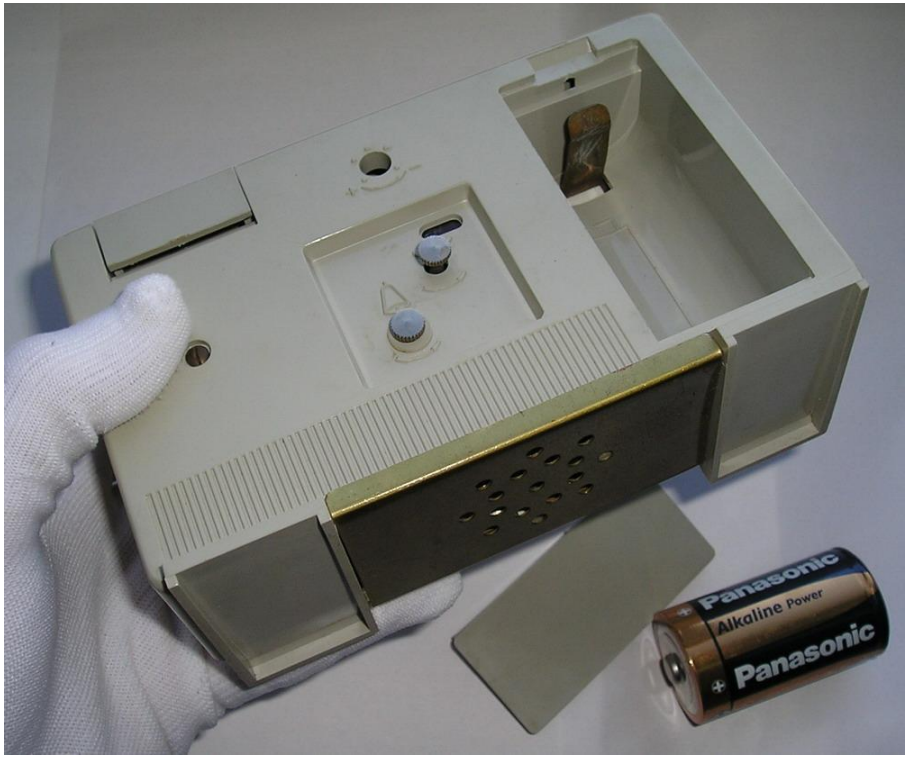
В случае, если закладное устройство имеет “глубокий камуфляж”, то надо в первую очередь **обращать внимание** на наличие элементов питания или разъёма для “зарядки” – *их не должно быть в механических часах*.



Осмотр предметов интерьера *(электромеханические часы)*.

Часы внимательно осматриваются как снаружи – на наличие подозрительных отверстий в корпусе и прикреплённых к нему посторонних предметов, так и изнутри – ***особое внимание*** обратить на различные внутренние полости.

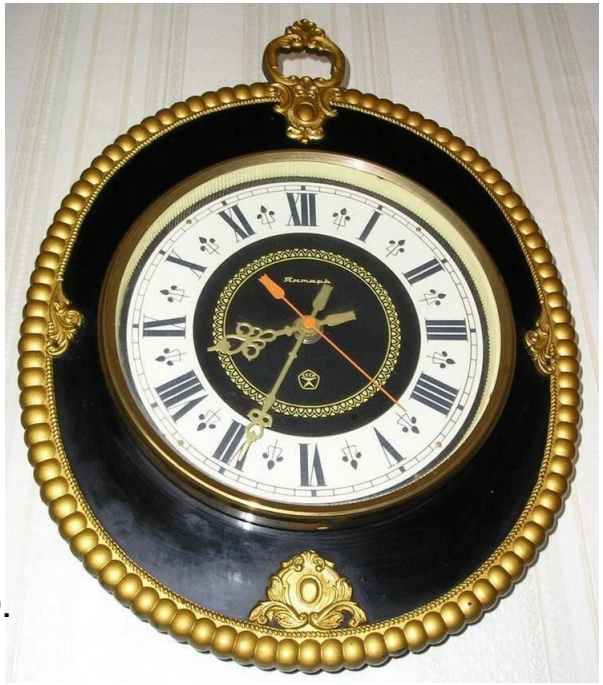
По возможности – *если есть соответствующая подготовка* – необходимо произвести разборку часов.



В электромеханических часах имеется свой “штатный” источник электропитания – *как правило, съёмная батарея*. Соответственно, таким часам не требуется ежедневный “завод” и владелец может не брать их в руки достаточно длительное время.

В случае, если закладное устройство имеет “глубокий камуфляж” *(в том числе “заводской”)*, то при осмотре надо обращать внимание на наличие ещё одного источника питания – *специально для “закладки”*, а так же на возможный “повышенный расход” штатной батареи – *если её приходится менять каждую неделю, то это должно “напрячь”*.

Осмотр предметов интерьера *(настенные часы)*.



С точки зрения злоумышленника настенные часы очень удобны для установки “заносных” средств съёма информации:
во-первых, они “висят высоко на стене” и их “не трогают”;
во-вторых, конструкция и габариты большинства настенных часов позволяют легко установить на их тыльной стороне диктофон или “заносной” радиомикрофон.

Кроме того, настенные часы часто используются для “глубокого камуфляжа” закладных устройств – как *аудио*, так и *видео*.

В подавляющем большинстве случаев настенные часы являются электромеханическими – *если конечно не брать настоящих ценителей, для которых настенные часы по определению должны быть только механическими и обязательно с гирями* – т.е. у таких часов есть “стрелки”, а источником электропитания является съёмная батарея.

Поэтому для них актуально всё, что было сказано ранее про осмотр электромеханических часов: *в частности, необходимо обращать внимание не только на наличие подозрительных отверстий в корпусе и прикреплённые к нему посторонние предметы, но и на наличие “дополнительного” питания*.

Пример осмотра *настенных часов, в которых установлена скрытая видеокамера*.

www.spyshop.cz

Закладное устройство выполнено “заводским” способом и имеет “глубокий камуфляж”. Видеозапись может осуществляться на встроенную память с последующим “скачиванием” или передаваться в режиме реального времени – *в обоих случаях используется Wi-Fi*.

Отверстие под видеокамеру можно обнаружить только при внимательном внешнем осмотре. Имеется два источника электропитания: съёмная батарея *(для “штатных” часов)* и встроенный аккумулятор *(для закладного устройства)* – это один из признаков возможного наличия встроенной “закладки”, на который надо обращать внимание при осмотре.

Пример осмотра *настенных часов, в которых установлена скрытая видеокамера*.

Закладное устройство выполнено “заводским” способом и имеет “глубокий камуфляж”.

Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени – *в обоих случаях используется Wi-Fi*.

Отверстие под видеокамеру можно обнаружить при внешнем осмотре.

На тыльной стороне часов имеются элементы, которые не характерны для обычных электромеханических часов: слот под карту памяти *(micro-SD)* и разъём mini-USB – *хотя имеется “штатная” батарея для питания часов*.

Наличие таких “не характерных” элементов должно сразу “напрячь”.

Осмотр предметов интерьера *(электронные часы)*.

В настоящее время электронные часы получили очень широкое распространение. Как правило, они “совмещены” с календарём, термометром и т.п., а иногда сами являются “элементом” более крупного электронного устройства – *например, музыкального центра*.

Фактически, **электронные часы можно считать “полноценной” бытовой электроникой и осматривать наравне с ней** – *см. далее*.

Очень часто источником питания в электронных часах является не съёмная батарея, а встроенный аккумулятор *(который периодически заряжается самим владельцем часов)* или они вообще постоянно “запитаны” от электросети – *поэтому если закладное устройство установлено внутри часов, то “проблем” с его электропитанием точно не будет*.

Электронные часы являются типовым вариантом для “глубокого камуфляжа” устройств съёма информации, выполненных “заводским” способом. В ряде случаев обнаружить такие “закладки” в ходе визуального осмотра может быть очень сложно или практически невозможно – *речь идёт о средствах “чисто акустического” контроля*. При этом такие изделия очень часто позиционируются производителями как “устройства охранного наблюдения” и в ряде стран продаются совершенно свободно или могут быть приобретены через “интернет-магазин”.

По возможности *(если есть соответствующая подготовка)* необходимо произвести разборку часов и нужно помнить, что для электронных часов очень актуально правило “**Учёт и контроль**”.

Пример *электронных часов, в которые “заводским” способом установлена скрытая видеокамера*.

www.spyshop.cz

Закладное устройство выполнено “заводским” способом и имеет “глубокий камуфляж”. Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени – *в обоих случаях используется Wi-Fi*.

Отверстие под видеокамеру находится за стеклянной “накладкой”, поэтому его можно обнаружить только при очень внимательном внешнем осмотре.

На тыльной стороне часов имеется разъём mini-USB – *для “зарядки”* встроенного аккумулятора, от которого “питаются” сами часы и встроенная в них “закладка”.

Так же имеется слот под карту памяти – один из признаков, указывающий на возможное наличие встроенного закладного устройства и который должен “напрячь” при осмотре.

Осмотр предметов интерьера *(игрушки)*.

Очень часто в проверяемом помещении могут находиться игрушки – *причём речь идёт не только о комнате отдыха или о детской, но и о рабочем кабинете*.

В ряде случаев, игрушка представляет собой не просто “*элемент интерьера*” или “*объект коллекционирования*”, а является очень дорогой *(не в материальном плане)* вещью для её владельца – *как правило, это память о близких и любимых людях или о безвозвратно ушедшем детстве*.

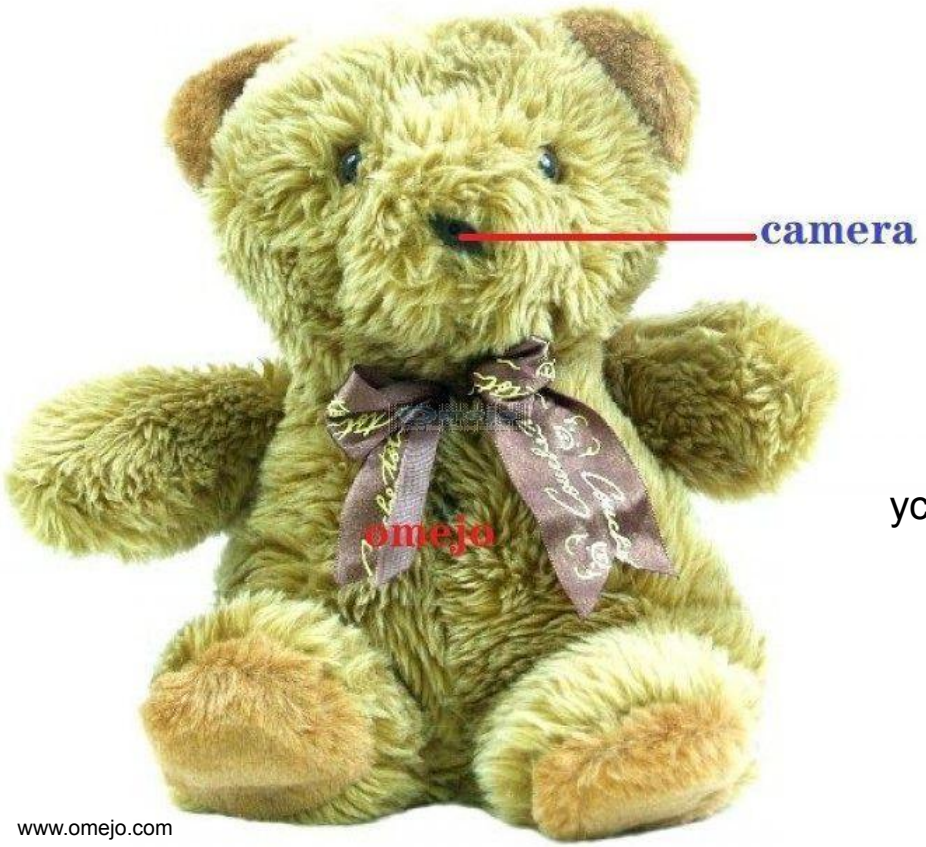
Классический пример такой игрушки показан в фильме “**Спрут**”: деревянная лошадка со сломанной ножкой, которую с детства хранил Тано Каридди – даже когда он стал миллионером.

Необходимо чётко понимать, что игрушки могут быть использованы злоумышленником для внедрения средств съёма информации *(аудио и видео)*.

В то же время, многие не воспринимают игрушки “всерьёз” – *в плане проведения их проверки*. Это неправильно и все игрушки должны быть проверены, как и другие предметы интерьера.

Осмотр предметов интерьера *(игрушки)*.

Злоумышленник может использовать имеющиеся в помещении игрушки для самостоятельной установки в них “простых” закладных устройств – *как правило, в виде “закрытого” модуля* – в первую очередь это касается использования диктофонов и “заносных” радиомикрофонов.



Другой вариант – это использование злоумышленником заранее приготовленной игрушки, в которой “заводским” способом установлено закладное устройство *(часто с ДУ)* – как правило, такие “игрушки” используются для скрытого видеонаблюдения. Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени – *в обоих случаях обычно используется Wi-Fi*.

Осмотр предметов интерьера *(игрушки)*.

Игрушки внимательно осматриваются и “прощупываются” на наличие каких-либо посторонних предметов, прикреплённых к игрушке или спрятанных внутри неё.

При наличии портативного металлодетектора будет очень полезно проверить с его помощью все игрушки, не содержащие металлических элементов.

Игрушки, имеющие в своём составе элементы “механики” и “электроники”, **должны разбираться для внутреннего осмотра**. “Полноценные электронные” игрушки, которых сейчас очень много, **можно считать бытовой электронной техникой** и **осматривать наравне с ней** – *см. далее*.

*Если в компании **случайно** имеется рентгенотелевизионная установка – например, по линии антитеррора – то все “подозрительные” игрушки на проверку.*

Осмотр предметов интерьера *(модели и аналогичные изделия)*.

В проверяемом помещении могут находится различные модели –
как собранные своими руками, так и купленные или подаренные.
При осмотре моделей нужно учитывать не только их конструкцию, но и их “происхождение”:
разбирается модель или она склеена “намертво”, собирали (покупали) вы её лично или вам её подарили уже в собранном виде и т.п. – от этого во многом зависит “глубина” осмотра.

Пример осмотра предметов интерьера *(собранные модели кораблей)*.

Модели, которые были собраны лично владельцем и которые по технологии изготовления склеены “намертво”, осматриваются снаружи на наличие прикреплённых к ним посторонних предметов – **особое внимание** обратить на различные открытые полости и подставку.

Осмотр предметов интерьера *(“готовые” модели)*.

Модели, которые были приобретены или подарены уже в “готовом” виде, необходимо осмотреть не только снаружи, но и внутри – *если есть такая возможность*. Очень часто “попасть внутрь” таких моделей без их физического повреждения практически невозможно – *поэтому полноценный визуальный осмотр таких изделий проблематичен*.

Осмотр предметов интерьера *(модели и аналогичные изделия)*.

На предыдущих слайда были рассмотрены только несколько вариантов наиболее простых *(в плане изготовления)* моделей.
В реальности, в проверяемом помещении могут находиться самые разные виды моделей, причём это могут быть не только отдельные изделия – *автомобиль, корабль, самолёт и т.д*., но и целые “объекты в миниатюре”, имеющие достаточно большие размеры и “штатное” электропитание – *например, модель аэропорта или вокзала, нефтяной вышки и т.п*.

Нужно понимать, что для полноценной проверки “сложных” моделей одного визуального осмотра может быть недостаточно, *так как в большинстве случаев никто не даст вам разбирать такую конструкцию “по винтикам”.* Качественно провести такую проверку сможет только опытный специалист, которому потребуется специальная поисковая аппаратуры.

В то же время, если говорить о “простых вариантах”, которые были рассмотрены ранее, то *для проверки моделей, не содержащих металлических деталей, будет очень полезен портативный металлодетектор*.

И нужно помнить про правило “**Учёт и контроль**” – конечно же “подмена” злоумышленником относительно крупной или “ломкой” модели маловероятна, но для небольших и компактных изделий такая угроза вполне реальна.

Осмотр “напольных” предметов интерьера.

Урны для мусора, напольные вазы и другие напольные предметы интерьера осматриваются внутри и снаружи – ***особое внимание*** *обратить на днища и на внутренние полости*.

Осмотр “напольных” предметов интерьера *(статуи)*.

Если в помещении имеются напольные статуи, то они внимательно осматриваются со всех сторон – *при необходимости нужно использовать досмотровые зеркала*.

В ходе осмотра **особое внимание** следует обратить на различные полости и “фигурные” элементы, в которых наиболее удобна установка “закладки”.

Осмотр предметов интерьера *(комнатные растения)*.

Декоративные комнатные растения *(среди которых есть настоящие “деревья”)* являются очень удобным местом для установки средств съёма информации. Необходимо внимательно осмотреть не только само растение, но и вазон, в котором оно находится *(снаружи и изнутри)*: в большинстве вазонов имеется система “дренажа”, которая включает в себя технологические полости *(пустоты)*. При “наружном” осмотре **особое внимание** обратить на изогнутый “ободок”, который есть вдоль верхней кромки большинства вазонов, и на “зазор” между днищем вазона и полом.

Осмотр туалета и ванной комнаты.

При осмотре туалета и ванной комнаты есть некоторые “нюансы”. Как правило, эти помещения могут быть использованы злоумышленниками для установки в них средств видеоконтроля – *для получения “компрометирующих” материалов в целях шантажа или для “иных целей” (если злоумышленник – “озабоченный” долб**б)*.

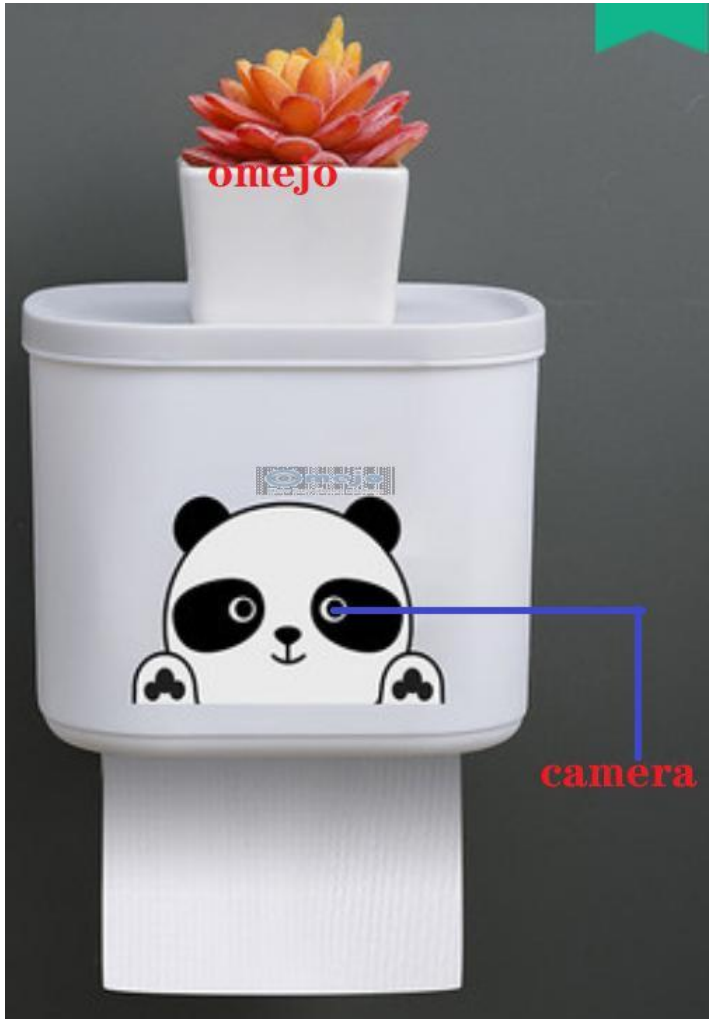
Осмотр туалета и ванной комнаты проводят по “типовой схеме”, как было изложено. В то же время, нужно отметить, что существует целый ряд устройств видеоконтроля, выполненных “заводским” способом и предназначенных для установки именно в этих помещениях – *такие изделия могут работать в условиях стопроцентной влажности и имеют **очень высокий** уровень камуфляжа*.

Поэтому при проверке туалета и ванной надо не только ориентироваться на поиск установленных в них “посторонних предметов” непонятного назначения, но и обратить особое внимание на осмотр находящихся в них “типовых” предметов: *держателей туалетной бумаги, мыльниц, баночек с кремом, шампуней и т.д*.

Все предметы интерьера внимательно осматриваются.
Если это возможно, то осуществляется их разборка или снятие с мест крепления – для внутреннего осмотра и для осмотра их тыльной стороны.

При наличии портативного металлодетектора будет очень полезно проверить с его помощью все объекты (мыльницы, баночки с кремом, шампуни и т.д.), не содержащие металлических элементов.

Осмотр предметов интерьера, находящихся в туалете и ванной.



www.omejo.com

Закладные устройства выполнены “заводским” способом и имеют “глубокий камуфляж”.

Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени по Wi-Fi.

Отверстие под видеокамеру можно обнаружить при внимательном внешнем осмотре.

Все предметы интерьера, находящиеся в туалете и ванной, внимательно осматриваются. Если это возможно, то осуществляется их разборка или снятие с мест крепления – *для внутреннего осмотра и для осмотра их тыльной стороны*.

Осмотр флаконов с туалетными принадлежностями.

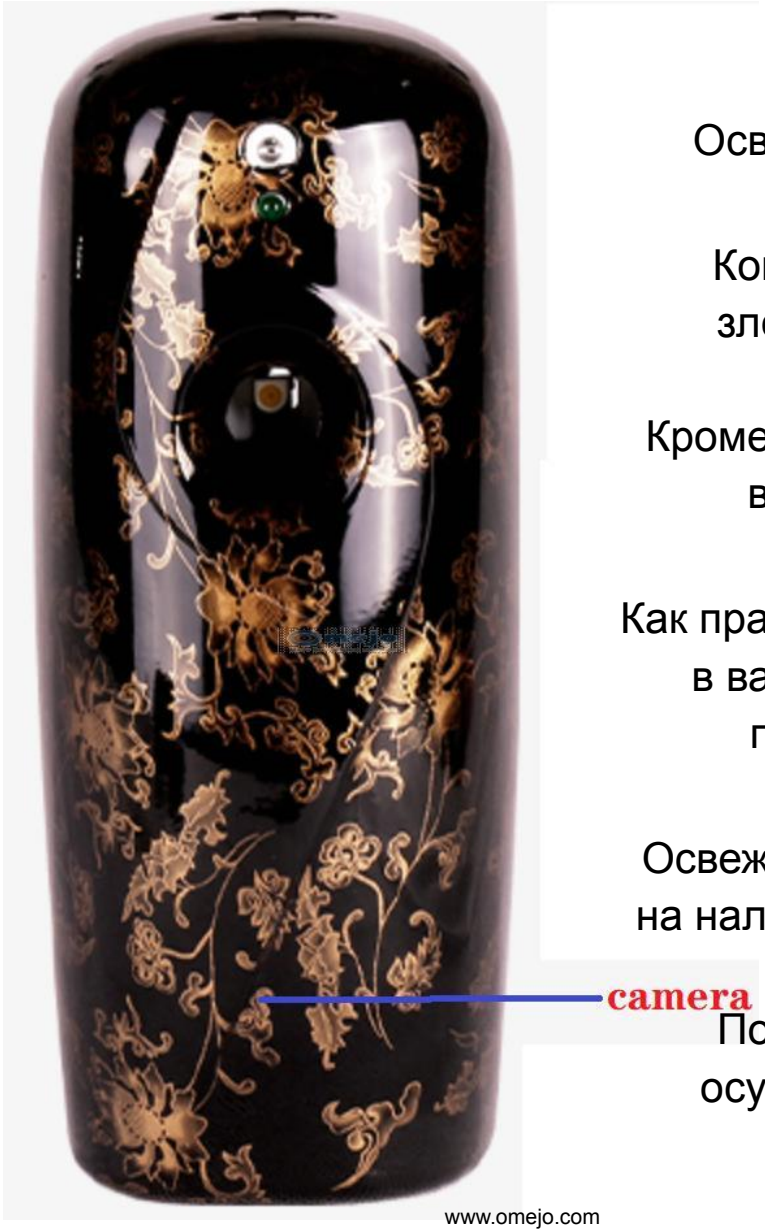
www.omejo.com

Закладные устройства выполнены “заводским” способом и имеют “очень глубокий камуфляж”. Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени по Wi-Fi.

Отверстие под видеокамеру можно обнаружить при очень внимательном внешнем осмотре.

Каждый флакон *(банка, туба и т.п.)* внимательно осматривается.

Особенности осмотра освежителей воздуха.



Освежитель воздуха является очень удобным местом для установки закладных устройств.

Конструкция большинства “освежителей” позволяет злоумышленнику самостоятельно установить в них устройства аудио- и видеоконтроля.

Кроме того, на базе “освежителей” существуют “закладки”, выполненные “заводским” способом и имеющие “глубокий камуфляж”.

Как правило, освежители воздуха устанавливают в туалете и в ванной комнате, но они могут находиться и в других помещениях – *например, в зале совещаний или в переговорной комнате*.

Освежители воздуха внимательно осматриваются снаружи на наличие прикреплённых к ним посторонних предметов и подозрительных отверстий в корпусе.

После этого производится разборка “освежителя” и осуществляется его тщательный внутренний осмотр.

www.omejo.com

Особенности осмотра “пищевой продукции” *(общие моменты)*.

Несколько слов по поводу осмотра объектов, связанных с “пищевой продукцией”. Если с осмотром непосредственно пищеблока *(как помещения)* всё более-менее ясно и его проверяют по “типовой схеме” *(как любое помещение) – включая и оборудование, которое там находится: кофе-машину, кухонный комбайн, электрочайник и т.д*., то при осмотре отдельных “элементов пищевой продукции” есть нюансы.

Очень часто при проверке не обращают внимания на пачки с печением, коробки конфет, бутылки с водой, пакеты *(банки)* с соком и т.п. – забывая основное правило: **каждый** предмет должен быть внимательно осмотрен.
Причём перечисленные выше предметы могут находиться практически в любых помещениях: в рабочем кабинете, зале совещаний, переговорной комнате и т.д.

Различные “элементы пищевой продукции” *(их упаковка)* могут быть эффективно использованы для камуфлирования средств съёма информации: это может быть как “самостоятельная” установка злоумышленником диктофона или радиомикрофона – *например, в коробку с конфетами*, так и использование закладных устройств, имеющих “глубокий камуфляж” и выполненных “заводским” способом.
Поэтому все “элементы пищевой продукции” должны быть внимательно осмотрены (естественно, речь не идёт о *“надкусывании”* и *“надламывании”* каждой конфеты).

При наличии портативного металлодетектора будет очень полезно проверить с его помощью все объекты (пакеты с соком, бутылки, коробки конфет и т.п.), не содержащие металлических элементов.

Пример осмотра “пищевой продукции”: видеокамера, установленная в бутылке для воды.

www.pimall.com

Закладное устройство выполнено “заводским” способом и имеет “очень глубокий камуфляж”.

Бутылка имеет “сборную” конструкцию и состоит из трёх отдельных модулей. Сама “закладка” находится в “среднем” модуле и скрыта за бутылочной этикеткой. “Верхний” и “нижний” модули абсолютно прозрачны и содержат в себе “вставки”, имитирующие воду. Визуально изделие выглядит как обычная бутылка с водой.

Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени – *в обоих случаях используется Wi-Fi*.

Как было сказано ранее, при проведение визуального осмотра помещения каждый находящийся там предмет нужно брать в руки и внимательно осматривать – в частности, бутылки с водой необходимо проверить на “прозрачность”, посмотрев через них “сверху вниз” или “снизу вверх”.

Пример осмотра “пищевой продукции”: видеокамера в кофейном стакане.

Закладное устройство выполнено “заводским” способом и имеет “глубокий камуфляж”.
Одноразовый кофейный стакан абсолютно обычный, а “закладка” находится в его “крышке”.
Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени –
в обоих случаях используется Wi-Fi.

www.pimall.com

Пример осмотра “пищевой продукции”: видеокамера в кофейном стакане.

Съёмная крышка внимательно осматривается на наличие каких-либо “нехарактерных” элементов: разъёмов, кнопок, переключателей и т.п.

В случае закладного устройства крышка будет “разборной” и будет состоять из основного модуля и “фальш-крышки”.

www.onlinespyshop.co.uk

Осмотр бытовой электронной техники *(некоторые общие моменты)*.

Осмотр бытовой электроники является очень важным элементом специального обследования помещения.

Как было сказано ранее, во многих случаях, характерных для “коммерческо-частного сектора”, устройства съёма информации могут быть установлены именно в бытовую электронику – *“самостоятельно” злоумышленником или “заводским способом”*.

В зависимости от того, какой вариант установки закладного устройства был использован – “*самостоятельный*” или “*заводской*”, будет принципиально отличаться вероятность его обнаружения при проведении визуального осмотра.

Как было уже отмечено *(моё личное мнение)*, **в ряде случаев** обнаружить установленную “заводским” способом “закладку” практически невозможно – *даже если разобрать для осмотра “штатное” электронное устройство* – если только проверка производится не в специализированной лаборатории.

Поэтому в отношении бытовой электроники очень важно правило: “**Учёт и контроль**” – данная техника должна приобретаться “случайным” образом в официальных магазинах, сразу после приобретения необходимо её проверить и взять “на учёт” *(“промаркировать”)*, а далее при проверках контролировать отсутствие “подмены” или несанкционированного “вскрытия”.

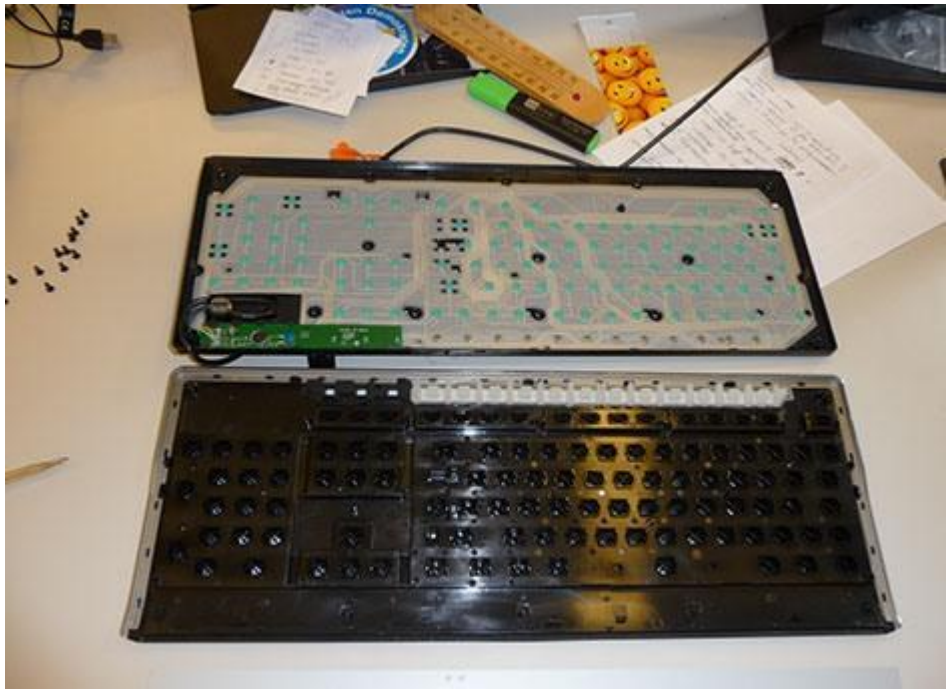
Осмотр бытовой электронной техники.

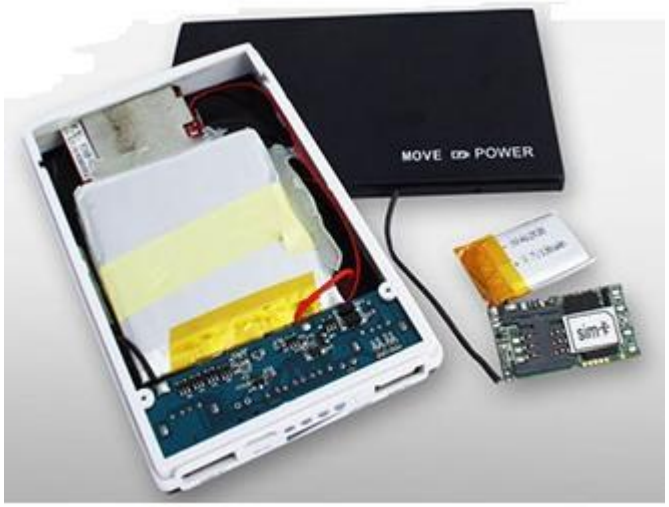
Осмотр электронной техники производится спокойно и тщательно, с обязательным соблюдением **правил электробезопасности**.

Человек, производящий осмотр бытовой электронной техники, должен обладать определёнными знаниями и навыками, позволяющими осуществлять вскрытие электронной аппаратуры и её осмотр изнутри.

Если такой подготовки нет, то лучше “не лезть во внутрь”, а **ограничиться внешним осмотром**:
в ряде случаев можно обнаружить следы возможного вскрытия, подозрительные отверстия в корпусе и т.д., а так же “внешние” устройства съёма информации *(см. далее)*.
В таких случаях для вскрытия электронной аппаратуры необходимо привлекать сотрудника подразделения информационных технологий.

Осмотр бытовой электронной техники.





www.storm-secure.de

Вскрытие электронной техники для её осмотра производится “поисковиком” только при наличии у него необходимой подготовки и соответствующих навыков. Если “поисковик” их не имеет, то вскрытие и осмотр электронной техники осуществляется совместно с сотрудником подразделения информационных технологий, обслуживающим её.

Осмотр бытовой электронной техники.

Как уже было сказано ранее, при осмотре бытовой электроники **необходимо обращать внимание на наличие каких-либо элементов, не характерных для данного типа техники**: если наличие *USB-разъёма* в музыкальном центре, телевизоре или в электронной фоторамке вполне логично и реально, то наличие слота для *SIM-карты* или для *карточки памяти* в электронных часах, зарядном устройстве или в калькуляторе сразу должно вызвать подозрение.

То же самое касается надписей, которые могут быть на кнопках и переключателях – например, если на электронных часах или калькуляторе имеется переключатель *“Rec” (On/Off)*, то это явный признак встроенного закладного устройства. И наоборот – наличие кнопок и переключателей непонятного назначения, которые не имеют никаких надписей, тоже должно “напрячь” и надо разбираться для чего они нужны.

При осмотре бытовой электроники **необходимо обращать внимание** на различные стеклянные поверхности *(экраны и т.п.)*, за которыми могут находиться скрытые видеокамеры – в первую очередь это касается закладных устройств, выполненных “заводским” способом и имеющих “глубокий камуфляж”.

Осмотр “современной” бытовой радиоэлектроники *(телевизоры, музыкальные центры и т.п.)*.

Большинство “современных” средств бытовой радиоэлектроники являются достаточно компактными и “плоскими”, что затрудняет “обычному” злоумышленнику возможность “самостоятельной” установки внутрь данной аппаратуры каких-либо средств съёма информации.

В то же время, практически вся “современная” бытовая радиоэлектроника имеет внешний USB-разъём, который может быть использован злоумышленником для некоторых устройств съёма информации. Кроме того, на базе “современной” бытовой электроники выполнено много “заводских” вариантов устройств съёма информации – *как правило, работающих в режиме “накопителя” или передающих информацию по Wi-Fi* – которые позиционируются их производителями как “охранные системы”.

Данная аппаратура внимательно осматривается снаружи на наличие подозрительных отверстий в корпусе и посторонних устройств, в том числе подключённых к USB-разъёму *(см. далее)*.
Если есть возможность, то производится вскрытие аппаратуры и её осмотр изнутри.

Осмотр “современной” бытовой радиоэлектроники *(телевизоры, музыкальные центры и т.п.)*.

www.onlinespyshop.co.uk

Проигрыватель DVD (CD) является одним из “типовых” вариантов установки средств съёма информации, выполненных “заводским” способом, – *как правило, это устройства видеозаписи*.

Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени – *в обоих случаях обычно используется Wi-Fi*.

При внешнем осмотре DVD-проигрывателя необходимо обратить **особое внимание** на различные отверстия и щели, которые имеются в его корпусе.

Если есть возможность, то необходимо произвести вскрытие и внутренний осмотр изделия.

Правило “**Учёт и контроль**” – обязательно!

Осмотр “классической” бытовой радиоэлектроники *(телевизоры, музыкальные центры и т.п.)*.

“Классическая” бытовая радиоэлектроника сейчас тоже встречается *(хотя и достаточно редко)*: *телевизоры с кинескопом, радиоприёмники, музыкальные центры в деревянных корпусах и т.п*. Такая техника является достаточно “объёмной” и наиболее вероятна “самостоятельная” установка в неё злоумышленником различных устройств съёма информации “модульного” типа – как с автономным питанием, так и “запитанных” от данной аппаратуры.

Данная аппаратура внимательно осматривается снаружи на наличие подозрительных отверстий *(щелей)* в корпусе и прикреплённых к корпусу посторонних предметов.
Если есть возможность снятия крышки корпуса *(разборки корпуса)*, то производится внутренний осмотр аппаратуры, в ходе которого обращается внимание на наличие подозрительных предметов и “непонятных” подключений.

Внимание!
Необходимо строго соблюдать правила электробезопасности!
Осматриваемая аппаратура должна быть не только “выключена” с помощью соответствующего тумблера или “кнопки”, но и “явно” отключена *(отсоединена)* от электросети.

Осмотр “классической” бытовой радиоэлектроники *(телевизоры, музыкальные центры и т.п.)*.

Осмотреть аппаратуру снаружи, обращая особое внимание на различные отверстия и щели. Все легкосъёмные элементы *(крышки и т.п.)* снимаются для осмотра внутренних полостей.

Осмотр “классической” бытовой радиоэлектроники *(телевизоры, музыкальные центры и т.п.)*.

При осмотре бытовой электроники особое внимание нужно обратить на различные “сетчатые” и “решётчатые” поверхности, которые часто присутствуют в конструкции радиоэлектронной аппаратуры – *в первую очередь, это связано с возможностью установки за ними скрытых видеокамер*.

https://mobilebooster.ru/post/209/skryitoe-videonablyudenie-kak-nayti-skryituyu-kameru

Осмотр бытовой электроники: пример “штатных” электронных устройств, в которых “заводским” способом установлены камера и микрофон.

www.onlinespyshop.co.uk

Высокий уровень камуфляжа.
Данные изделия могут работать как в режиме “чистого накопителя” – записывая аудио- и видеоинформацию в память, так и осуществлять “промежуточное” накопление информации с последующей её передачей по радиоканалу *(обычно через Wi-Fi)*.

Осмотр бытовой электроники: пример “штатных” электронных устройств, в которых “заводским” способом установлены камера и микрофон.

Многие устройства такого типа позиционируются производителями как “охранные системы” и в ряде стран могут быть приобретены совершенно свободно или заказаны через “интернет-магазин”.

В ряде случаев могут отсутствовать “явные внешние признаки”, указывающие на наличие внутри “штатного” электронного устройства каких-либо средств съёма информации – *за исключением отверстия для камеры (иногда и для микрофона)* – при этом всё управление осуществляется с помощью “штатных” кнопок “основного” устройства. В то же время, в некоторых случаях на корпусе “основного” (*“штатного”*) устройства могут быть различные элементы, не характерные для электроники такого типа: слот для карты памяти, кнопки и переключатели непонятного назначения и т.п. – на всё это **нужно обращать внимание при осмотре**.

Осмотр бытовой электроники: пример “штатных” электронных устройств, в которых “заводским” способом установлена видеокамера.

Видеорегистратор с модулем Wi-Fi установлены в обычной Bluetooth-колонке. Видеозапись может осуществляться на карту памяти с последующим “скачиванием” или передаваться в режиме реального времени по Wi-Fi.

www.onlinespyshop.co.uk

Очень высокий уровень камуфляжа. Bluetooth-колонка полностью сохраняет все свои “штатные” функции и полноценно работает. На колонке отсутствуют какие-либо специальные кнопки или переключатели для управления видеорегистратором – *всё осуществляется с помощью “штатных” кнопок*.

Питание закладного устройства осуществляется от штатного аккумулятора колонки, который периодически заряжается самим владельцем.

Камера за “решёткой” может быть обнаружена при внимательном внешнем осмотре.

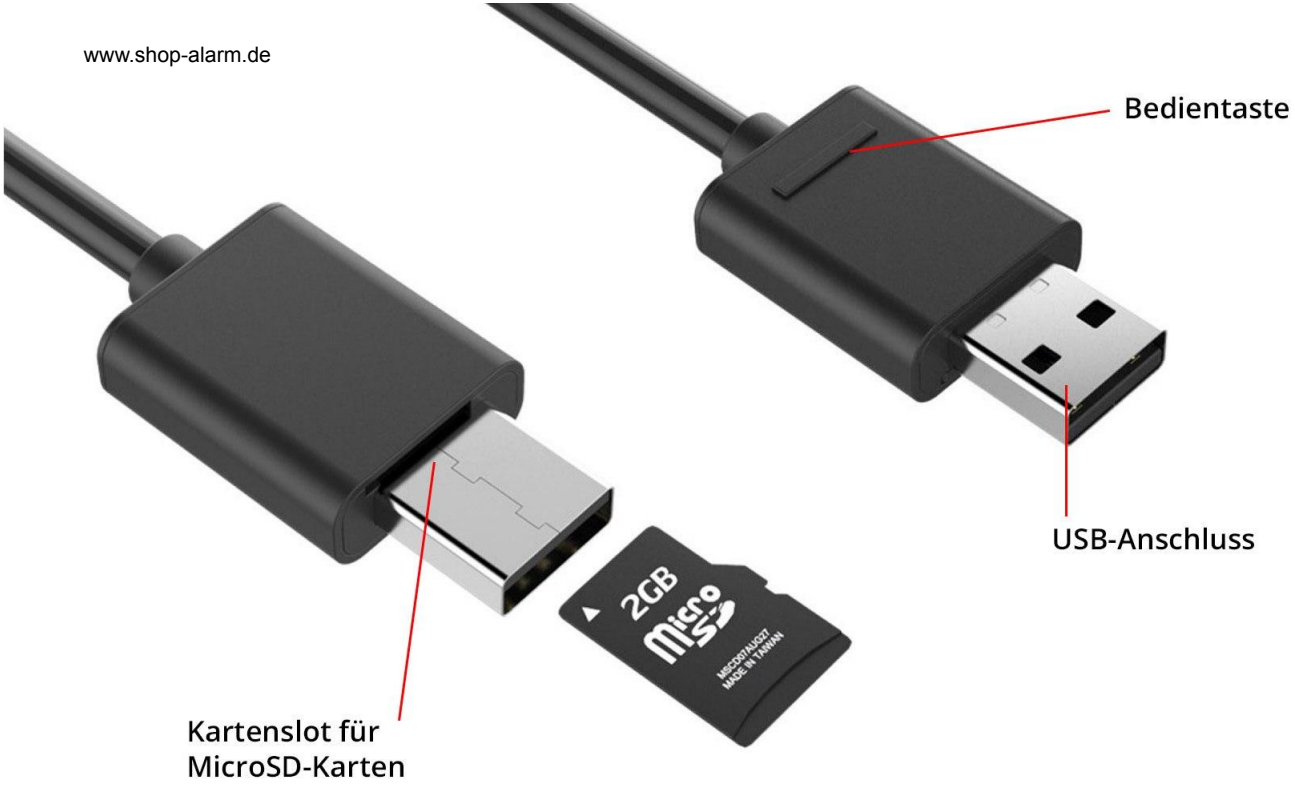
Осмотр электроники, имеющей USB-разъём.

Как было сказано ранее, одними из наиболее вероятных технических средств съёма информации, которые могут быть использованы в “коммерческо-частном” секторе, являются диктофоны и GSM-передатчики. При этом, существуют GSM-передатчики и диктофоны, которые подключаются к штатным USB-разъёмам: в компьютере, телевизоре, музыкальном центре и т.д.

Такое устройство, подключённое злоумышленником к электронной технике в “нужном помещении”, может работать практически неограниченное время – пока не будет обнаружено.

Поэтому <u>все USB-разъёмы осматриваются на наличие каких-то “левых” флэшек и кабелей</u> – *в ходе осмотра обязательно взаимодействие с сотрудником подразделения информационных технологий, обслуживающим данную технику*.

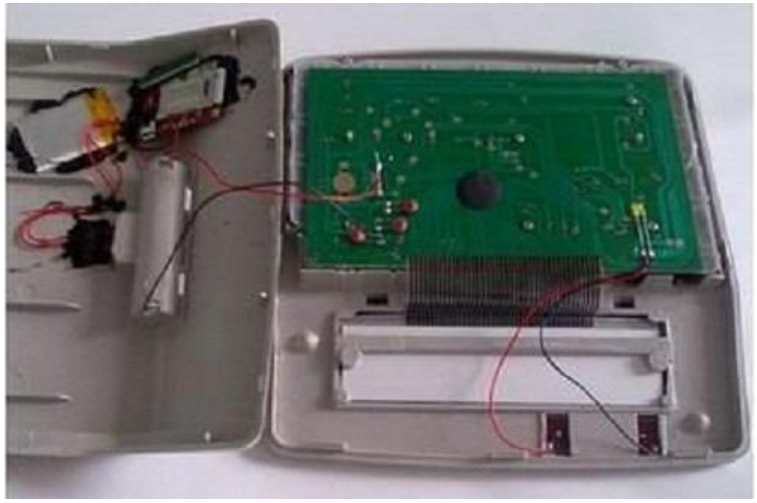
Пример диктофона, закамуфлированного в USB-кабеле.



Внимание!

При возникновении каких-либо вопросов, связанных с осмотром штатной электронной техники, необходимо проконсультироваться с сотрудником подразделения информационных технологий, который её обслуживает.

Пример “самодельного” GSM-передатчика, установленного в калькулятор.



Имеется целый ряд “подозрительных” признаков, которые могут быть выявлены при внешнем осмотре: слот для SIM-карты, разъём для подключения зарядного устройства *(для аккумулятора)*, кнопка управления (включение/выключение).

Все эти “явные” признаки должны быть замечены при визуальном осмотре.

www.spymarket.info/shop/261/desc/kalkuljator-casio-gsm-zhuchok-proslushki

Пример “заводского” GSM-передатчика, установленного в калькулятор.

Высокий уровень камуфляжа: внешне нет практически никаких “явных” признаков – только два “накола” на боковой поверхности корпуса, через которые звук поступает на микрофон и осуществляется управление передатчиком (включение/выключение). Для зарядки аккумулятора нужно разбирать калькулятор и подключать зарядное устройство “внутри”, слот для SIM-карты тоже находится “внутри”.

www.onlinespyshop.co.uk

Наличие “наколов” в корпусе – один из моментов, на которые нужно обращать внимание при проведении визуального осмотра предметов. Обнаружение “накола” сразу должно “напрячь”.

Осмотр бытовой электроники: *пример GSM-передатчика, закамуфлированного в “мышь”*.

Высокий уровень камуфляжа: внешне нет практически никаких “явных” признаков закладного устройства. При этом “мышь” сохраняет все свои “штатные” функции и полностью работоспособна.

Питание передатчика осуществляется от ПК через штатный USB-разъём – *главное, чтобы компьютер был включён*.

Как было ранее сказано, для проведения работ по проверке средств вычислительной техники, предусматривающих её разборку, у “поисковика” должна быть соответствующая подготовка. Если такой подготовки нет, то разборку средств вычислительной техники необходимо производить совместно с сотрудником подразделения информационных технологий.

Правило “**Учёт и контроль**” – обязательно!

Осмотр телекоммуникационного оборудования на наличие различных “дополнительных” функций.

Как было сказано ранее, некоторые модели телекоммуникационного оборудования могут иметь ряд “штатных” возможностей и, так называемых, “дополнительных” функций, которыми может воспользоваться грамотный злоумышленник как для перехвата информации, циркулирующей в телекоммуникационных сетях – *это касается офисных мини-АТС и систем IP-телефонии*, так и для получения аудио- и видеоинформации из помещений, в которых находятся соответствующие абонентские устройства *(телефонный аппарат, факс и т.д.)*.

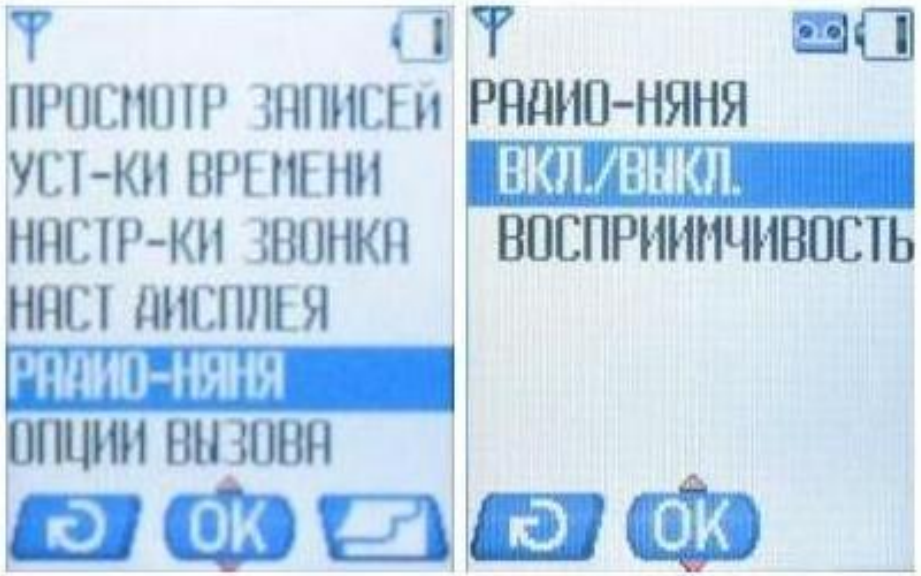
Ещё раз нужно отметить, что речь идёт не о внедрении “программных закладок”, а об использовании именно “штатных” функций: *“Вклинивание в разговор” , “Запись в систему голосовой почты”, “Room Monitoring” и т.д*.

Для выявления таких “дополнительных” функций **необходимо тщательно изучить техническую документацию** на конкретную модель мини-АТС и на соответствующее абонентское оборудование.

Данная работа осуществляется **совместно с представителем подразделения информационных технологий**, обслуживающим телефонную сеть.

При этом нужно чётко понимать, что основную роль в обнаружении таких угроз играет именно **грамотный** сотрудник подразделения информационных технологий и если такого человека в компании нет, то дело плохо…

Осмотр абонентского телекоммуникационного оборудования (телефонов DECT) на наличие различных “дополнительных” функций.



В случае регистрации ещё одной трубки пользователь получает в свое распоряжение режим "Няня" для прослушивания удаленного помещения.
С помощью этой функции можно слышать, что происходит в комнате, в которой находится другая трубка.
Хотя, трудно предсказать, с какими целями можно использовать эту функцию, например, в офисе...

Во многих беспроводных телефонах (в частности, стандарта DECT) есть возможность использования абонентской трубки в режиме “радио-няня” *(фактически радиомикрофона)* – если на данной трубке был предварительно активирован данный режим.

Для выявления такой угрозы **необходимо тщательно изучить техническую документацию на конкретную модель телефона**. Данная работа осуществляется совместно с представителем подразделения информационных технологий, обслуживающим на объекте телефонную сеть.

Осмотр персональных компьютеров, ноутбуков, “планшетов” и т.п.

Моё личное мнение: компьютер, у которого есть “штатный” микрофон и видеокамера, уже “по определению” является **диктофоном** или **видеорегистратором** – *даже без установки в него каких-либо “специальных” устройств съёма информации*.

Кроме того, если компьютер имеет кабельное подключение к локальной сети или к Internet, то его можно рассматривать в качестве “**проводной закладки**”,
А если у компьютера имеется модуль *Wi-Fi (Bluetooth, 3G, 4G и т.п.)*,
он фактически становится “**радиозакладкой**”.

При этом возможны два варианта, позволяющих использовать обычный компьютер в качестве устройства съёма информации: внедрение в него специальных “программных закладок” или использование некоторых “штатных” программ, имеющих ряд определённых “особенностей” – например, *“Автоматический ответ” при входящем звонке в Skype*.

На мой взгляд, наибольшую опасность представляют именно “программные закладки”, обнаружить которые очень сложно.

Поиск “программных закладок”, внедрённых в вычислительную технику и телекоммуникационное оборудование.

Как было сказано ранее, **очень серьёзная угроза** связана с применением т.н. “программных закладок”, которые могут быть внедрены злоумышленником в средства вычислительной техники и в телекоммуникационное оборудование.

В этом случае ваш “родной” компьютер, “планшет”, смартфон и т.п. переходит под дистанционное управление злоумышленником и фактически становится устройством съёма информации – причём для получения информации используются его “штатные” микрофон и видеокамера.

На мой взгляд, с развитием современных технологий эта угроза становится всё более и более актуальной и реальной:

Во-первых, зачем злоумышленнику рисковать, чтобы что-то “занести” на объект, когда он может с успехом использовать в своих целях “штатную” технику, которая совершенно легально находится на объекте *(например, компьютер)* или вообще непосредственно “в кармане” у интересующего лица *(смартфон)*.

Во-вторых, в последнее время появляется всё больше “программных закладок” – *в том числе достаточно серьёзных (типа “Pegasus”)*, которые активно используются злоумышленниками в “коммерческо-частном секторе”.

Ещё раз повторю: речь идёт о “программных закладках”, которые позволяют не только организовать утечку хранящихся и обрабатываемых данных – *это само собой*, но и “превратить” абонентские терминалы в “подслушивающие устройства”.

Поиск “программных закладок”, внедрённых в вычислительную технику и телекоммуникационное оборудование.

Естественно, что ***в ходе проведения визуального осмотра помещения невозможно обнаружить угрозы****, связанные с “программными закладками”, внедрёнными в “штатное” оборудование (в том числе и т.н. “телефоны-шпионы”)*. Для выявления этих угроз необходима плановая совместная работа подразделения информационных технологий и подразделения, отвечающего за вопросы ТЗИ, **сотрудники которых должны иметь специальную подготовку**.

Необходимо чётко понимать, что основную роль в обнаружении таких угроз играет именно **грамотный** сотрудник подразделения информационных технологий и если такого человека в компании нет, то дело плохо…

Понятно, что обнаружение “программных закладок” по своей специфике больше относится к тем вопросам информационной безопасности, которые находятся в компетенции подразделения информационных технологий – по аналогии с “антивирусной” защитой.

При этом, сотрудники, отвечающие за вопросы технической защиты информации, должны чётко представлять себе возможность таких угроз и стараться максимально противодействовать им *(в первую очередь, с помощью т.н. “организационных” мер)*: от элементарного закрытия *(“заклеивания”)* камеры ноутбука – *если она не используется в данный момент*, до разработки и реализации процедуры использования средств вычислительной техники и связи на объекте.

Небольшой “итог”, связанный с визуальным осмотром помещения.

Вот вкратце *(хотя получилось “совсем не вкратце”)* основные моменты, связанные с проведением визуального осмотра помещения в целях выявления возможно внедрённых средств съёма информации: вроде бы всё *“просто”* и *“легко”*, но на самом деле это кропотливая и достаточно сложная работа.

Ещё раз повторю, что всё, о чём я говорил – это элементарные базовые вещи, которые известны любому, кто имеет соответствующую подготовку и пытается **реально** заниматься вопросами технической защиты информации – *в частности, поиском устройств съёма информации*.
Такие люди не узнают для себя ничего нового из моей презентации – *они и так всё это знают лучше меня*.

В то же время, для большинства **граждан, не имеющих какой-либо подготовки в этой области** *(именно на них была рассчитана данная презентация)*, многие рассказанные вещи могут быть достаточно полезными.
Надеюсь, что презентация поможет им взглянуть на вопросы ТЗИ *“по-новому”*, развеет имевшиеся у них *“фильмово-фантастические” представления* и “подтолкнёт” их более реально задуматься над данной проблемой.

Тут можно вспомнить старую пословицу:
“Один искренне раскаявшийся грешник ценнее, чем десять праведников”.

Основное, что надо чётко понимать и помнить: не существует *“чудо-приборов”*, а есть планомерная и осознанная работа – только она может дать реальный результат.

Небольшой “итог”, связанный с визуальным осмотром помещения.

Учитывая, что значительная часть аудитории, на которую была рассчитана данная презентация – это бывшие “силовики”, в настоящее время являющиеся сотрудниками частных служб безопасности и личной охраны, хочу подчеркнуть необходимость максимального использования имеющегося у них опыта предыдущей службы: *инженерно-сапёрной подготовки у бывших “армейцев” или осмотра места происшествия (проведение обыска) у бывших “правоохранителей”* – эти навыки нужно просто “перенаправить” на решение задач по поиску устройств съёма информации *(после определённой “переподготовки” в этом направлении)*.

Естественно, что речь идёт только об адекватных и думающих людях, которые могут самостоятельно развиваться и решать новые задачи.

В то же время, существует категория индивидуумов, которых бесполезно чему-то учить или переучивать – они живут *(причём неплохо живут)* по принципу: *“Не переживай! Пока поймут, что ты дебил, ты будешь уже капитан. Пока решат, что с тобой дальше делать, ты майор и у тебя уже есть пенсия”*.

Вот некоторые примеры *“работы”* таких *“работников”*:

https://drive.google.com/file/d/1yOSaiBC63ZHEEWksNDS9vTaeVp_Dr5dg/view?usp=sharing

Понятно, что бестолковые люди будут всегда и с этим ничего не поделаешь. К сожалению. А может быть наоборот – к счастью… Вопрос “философский”.

Небольшое заключение – *для “заказчиков” и “хозяев” (“работодателей”).*

Несколько слов в заключение данной презентации – для тех, кто не смотря ни на что *(имеется ввиду “занудность” моей презентации)*, всё-таки смог “осилить” её до конца и не заснул, не разбил компьютер, не ушёл в запой или не застрелился из личного оружия *(у кого оно есть)*.

Для *“заказчиков”* и *“хозяев” (“работодателей”)*, на мой взгляд, можно сказать одну основную фразу: “***Граждане “заказчики”, не будьте лохами!***” – это касается как приглашения “человека со стороны” для проведения специальной проверки вашего объекта, так и кадровых вопросов, касающихся соответствующих работников вашей компании.

Как было сказано, конечно же “заказчик” или “владелец компании” не могут и не должны полноценно разбираться в вопросах защиты информации. Но обыкновенное здравомыслие и элементарные знания из школьного курса физики должны быть у всех – этого, *на мой взгляд*, вполне достаточно, чтобы не попасть на *“развод”*, когда вас будет *“грузить”* рассказами о *“чудо-приборах”* и *“высоких технологиях”* приглашённый со стороны *“крутой специалист”*.

Что касается выявления непрофессионального работника *(“работника-дурака”)*, работающего в вашей компании и *“имитирующего бурную деятельность”*, то это более сложная проблема, но и она при желании может быть решена.

Небольшое заключение – *для “начинающих работников” в области ТЗИ*.

Для “работников”, которые **начинают** заниматься вопросами защиты информации, хочу повторить несколько важных *(на мой взгляд)* моментов:

Во-первых, как говорил В.И.Ленин – необходимо *“**Учиться, учиться и учиться**”*. Речь идёт не только об **обязательной начальной подготовке** – *это само собой*, но и о **постоянном самостоятельном развитии** непосредственно в ходе работы. Причём понимание необходимости в постоянном обучении должно быть у самого сотрудника и он сам должен искать и использовать все возможности для учёбы.

Типовая ситуация: многие *“работники”* тупо сидят годами ничего не делая – *как говорится, околачивают груши определёнными частями тела* – при этом постоянно жалуются друг-другу, что их не отправляют на учёбу за рубеж, не повышают им зарплату и вообще не ценят *“таких крутых специалистов”*. А если посмотреть реально, то эти “*крутые специалисты*” не только ничего не умеют, но даже не понимают, чем они вообще должны заниматься.

Приходилось встречаться со *“специалистами”* (кавычки!), которые за несколько лет своей, *с позволения сказать* “*работы*”, не только ни разу не включили имевшийся у них анализатор проводных линий, но даже не прочитали *(вообще не открывали)* инструкцию на данное изделие – *кстати, никакую специальную литературу за это время они тоже не прочитали, а литература была и очень хорошая*. Вот уж действительно наглядное подтверждение поговорки: *“**Учиться** никогда не поздно, но **иногда – бесполезно**”*.

Небольшое заключение – *для “начинающих работников” в области ТЗИ*.

В то же время, **нужно чётко понимать**, что для **реальной работы** с некоторыми видами поискового оборудования кроме прохождения кратковременных курсов по технической защите информации **необходимо** иметь базовое техническое образование в области радиотехники или связи.

Например, работа с комплексами радиоконтроля: кто-то думает, что это *“легко и просто”* и он этому *“быстро научится”*, став *“крутым оператором”* за неделю *(максимум за месяц)*. Естественно, что это бред и всё совсем не так – *см. несколько следующих слайдов*.

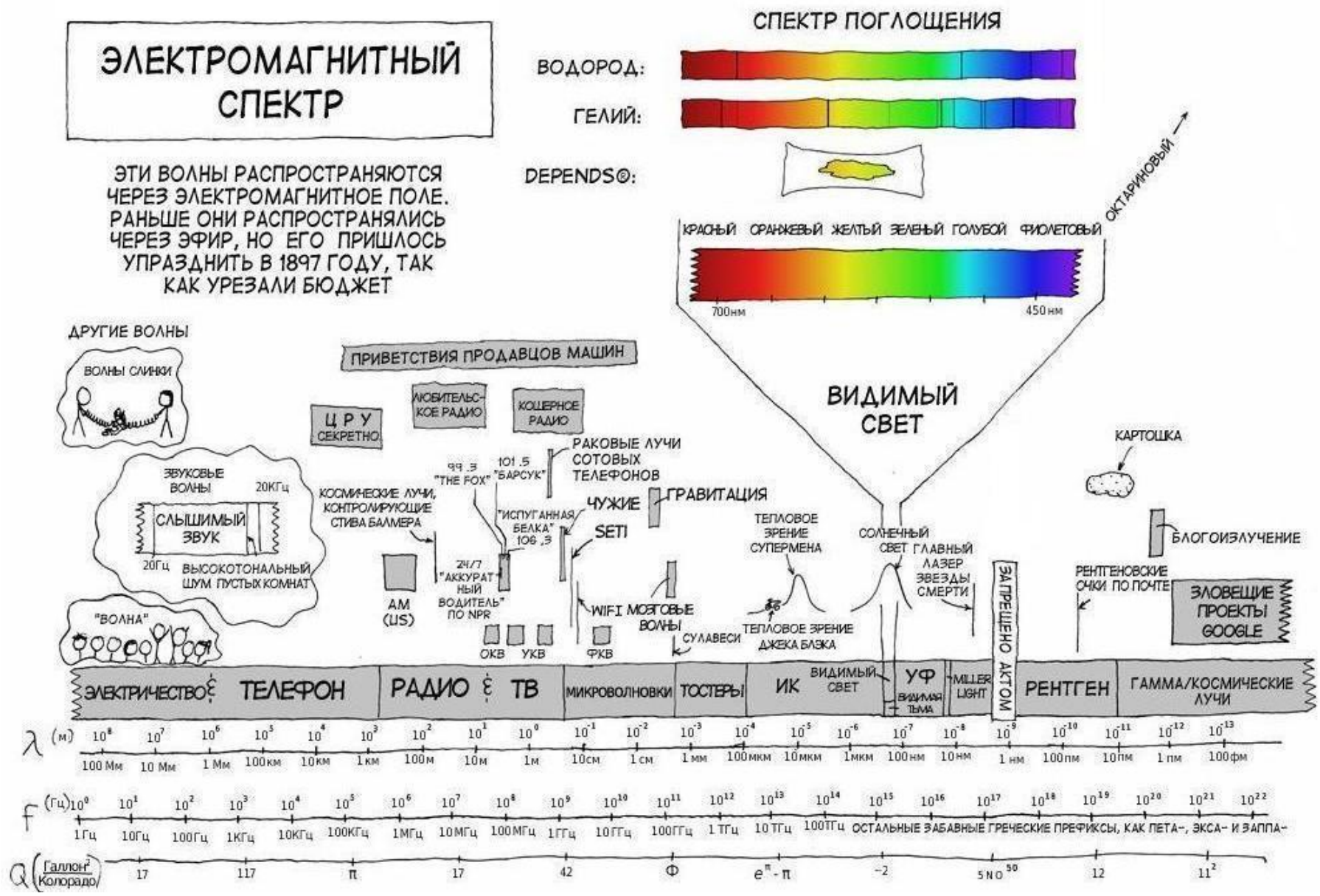
Моё личное мнение: без соответствующего базового образования практически нереально освоить **полноценную работу** с **настоящим комплексом** радиоконтроля – даже съездив на двухнедельные курсы по подготовке “специалистов в области защиты информации” *(естественно, речь не идёт о различных “показных” вариантах, имитирующих работу)*.

И наоборот: человек, имеющий хорошую “базовую подготовку” в области радиотехники *(я имею ввиду реальные знания, а не просто “корочку” об окончании учебного заведения)*, сможет самостоятельно освоить **основы** работы практически с любым комплексом радиоконтроля *(если на него есть грамотная подробная инструкция)* – ну а дальше, как очень хорошо было сказано на форуме: *“Развиваться, насколько ума хватает”*. Понятно, что по каким-то возникающим вопросам нужно будет консультироваться с производителем или с “опытным пользователем” *(как правило, можно и “удалённо”)*.

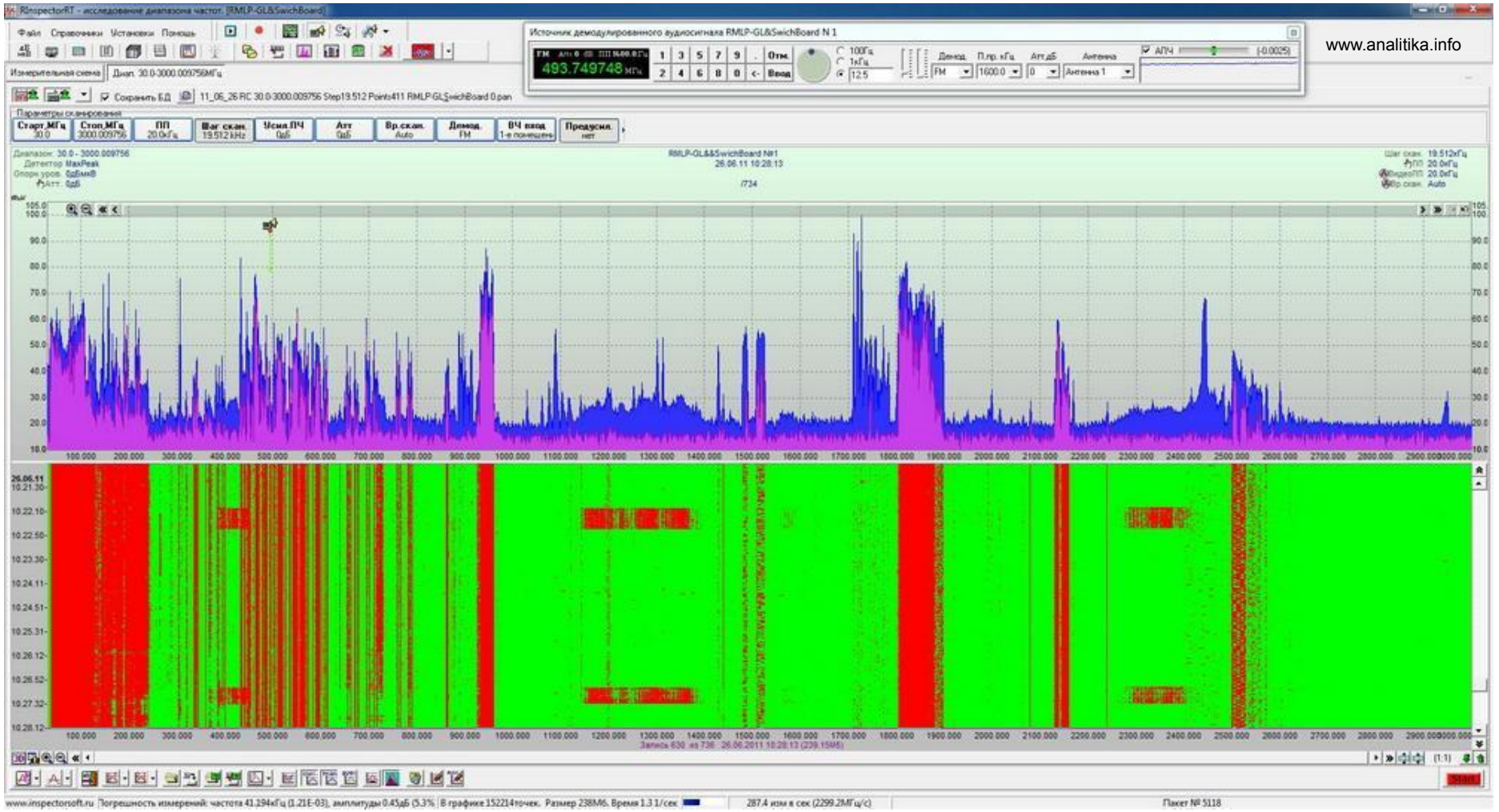
Примечание: естественно, что данный человек должен сам хотеть научиться работать с комплексом – иначе никакого результата не будет, *даже если у него есть хорошая “база”*.

“Неформальная” модель частотного спектра.

Примерно такое представление о *“волнах”*, *“частотах”* и других *“непонятных вещах”* имеют многие граждане, *далёкие от знания физики*, но считающие себя *“продвинутыми в технике”*.



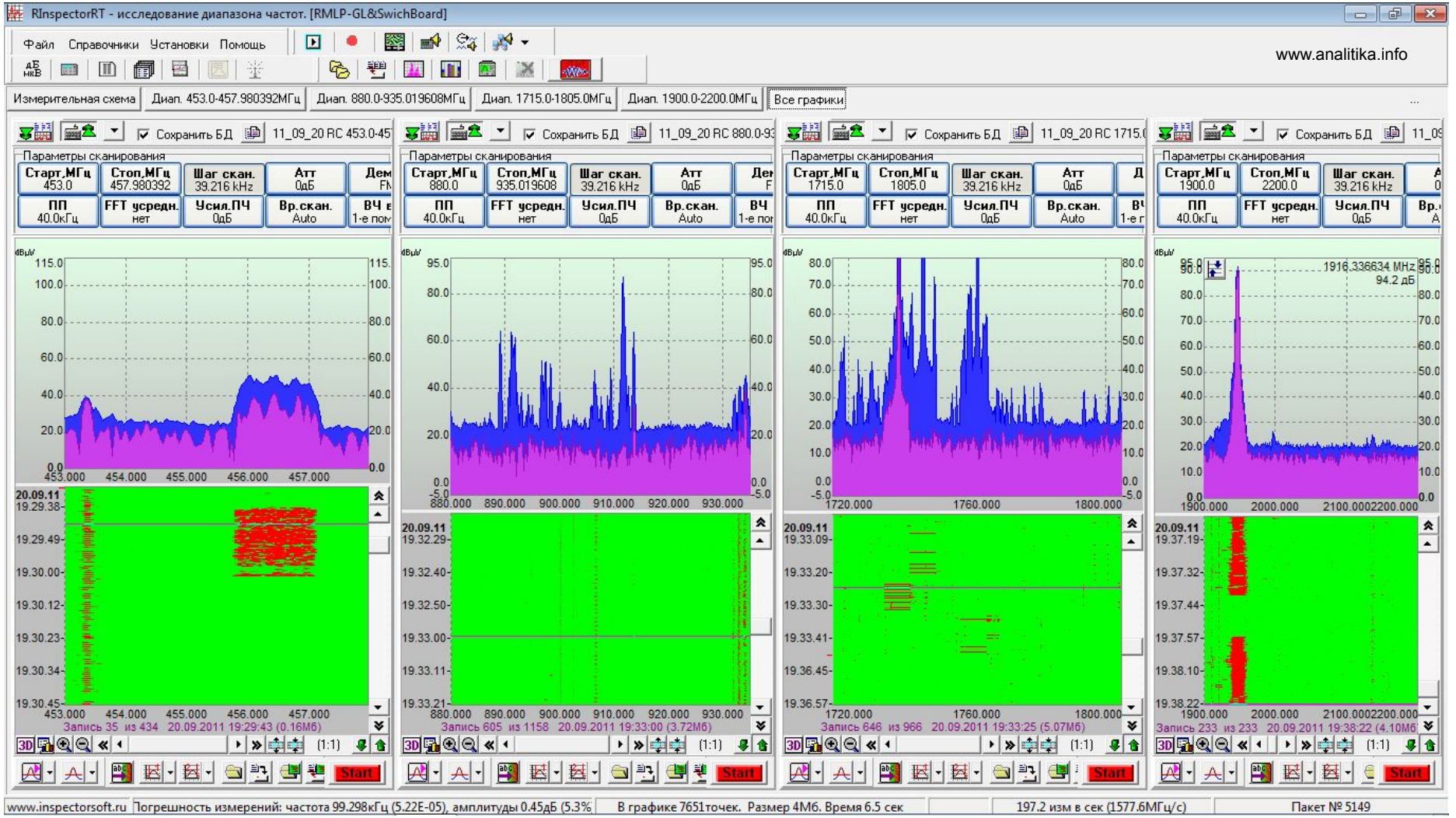
Пример реальной картины, которая появится на экране комплекса радиоконтроля.



Именно такую картину увидит оператор на мониторе комплекса радиоконтроля или анализатора спектра – *графика будет отличаться в зависимости от конкретной модели оборудования, но в целом "первое впечатление" будет примерно таким*.

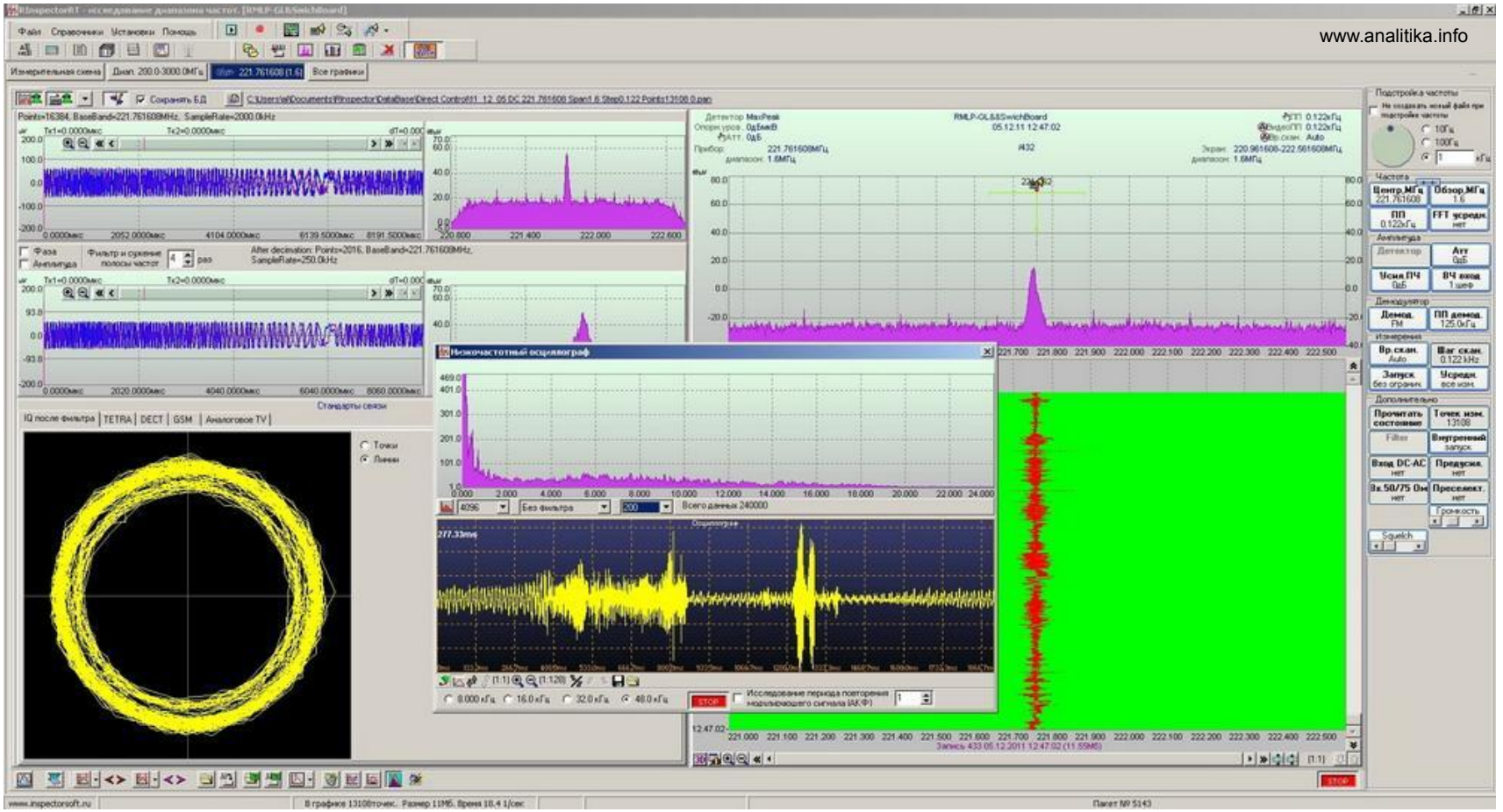
Но это – **только начало**, и оператор должен знать и уметь, что с *"этим"* делать дальше.

Примеры исследования отдельных участков частот.



В ходе дальнейшей работы с комплексом радиоконтроля потребуется исследование отдельных диапазонов частот – в частности тех, в которых были обнаружены “подозрительные” сигналы или в которых наиболее вероятна работа “радиозакладок”.

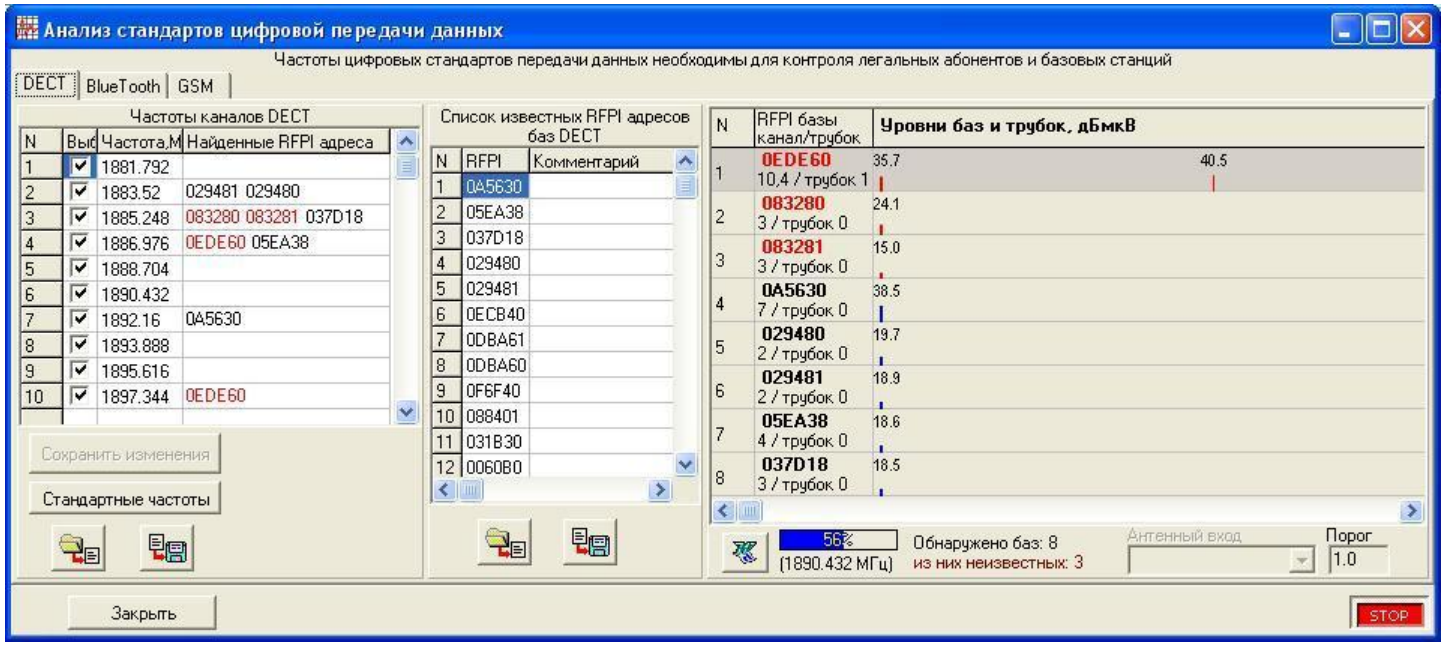
Пример анализа конкретного *“подозрительного”* радиосигнала.



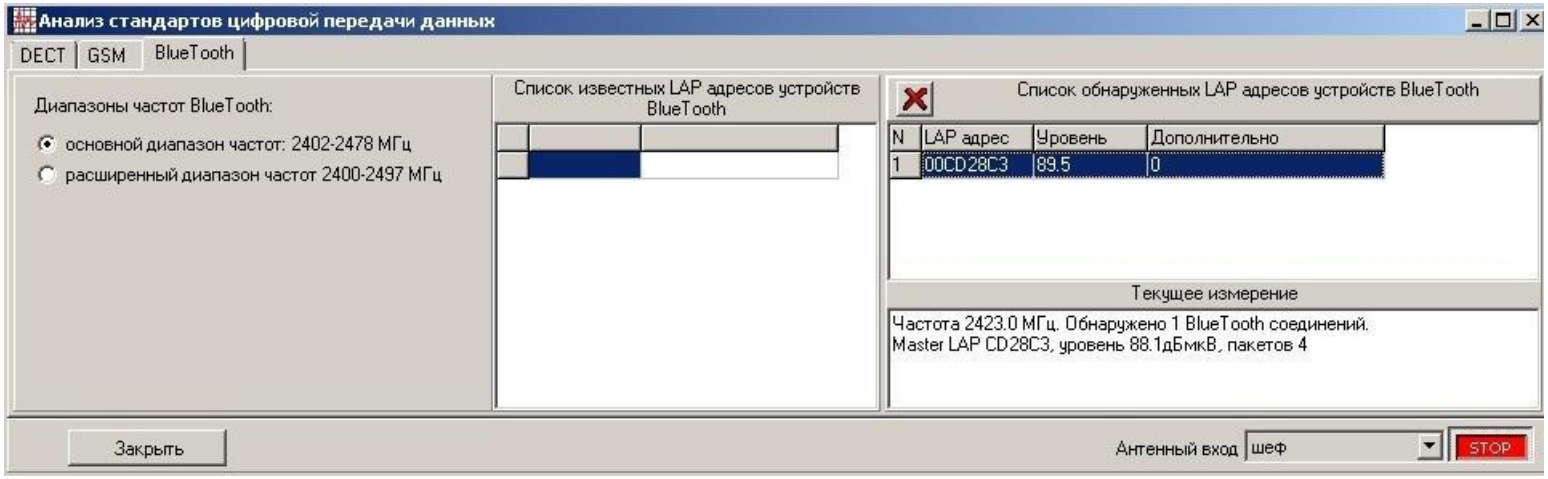
А далее – *если это позволяет оборудование* – оператор должен будет провести детальный комплексный анализ каждого сигнала, который он посчитает “подозрительным”.

Естественно, что вся эта **работа должна быть** “**осознанной**” и **оператор должен чётко понимать, что он делает** и **зачем**, а не просто тупо *“нажимать кнопки” и “крутить ручки”* – что обычно и происходит среди недоучек, которые *“имитируют бурную деятельность”*.

Пример анализа работы устройств стандартов DECT и Bluetooth .



www.analitika.info



Анализ стандартов цифровой передачи данных – это вообще *“отдельная история”*.
Для этого необходимо знать не только *“физику”*, но и *“логику”* работы данных систем.

Небольшое заключение – *для “начинающих работников” в области ТЗИ*.

Вот такие *“страшные”* и непонятные для обычного человека картинки можно увидеть при работе с комплексом радиоконтроля – *аналогичная ситуация будет при работе с серьёзным анализатором проводных линий (типа **TALAN**) и другой техникой*.

Так что ещё раз хочу повторить *(моё личное мнение)*: для человека, не имеющего **реальных базовых знаний** в определённых областях – *именно **реальных** знаний, а не “корочки” о прохождении учёбы и не “стажа работы”* – научиться **реально работать** с такого рода оборудованием практически невозможно.

Все разговоры о том, что *“крутой комплекс радиоконтроля сам обнаружит закладку”* и *“оператору вообще ничего не надо делать, только его включить”* – это полный бред.

Кроме того, если речь идёт об организации реального радиоконтроля, а не о его имитации, то в компании должен быть отдельный подготовленный человек, который будет заниматься только этим вопросом – естественно, что такое “удовольствие” могут позволить себе только очень серьёзные структуры.

Что касается ситуации, характерной для абсолютного большинства молдавских компаний, *когда вопросами технической защиты информации поручено заниматься “в нагрузку” кому-нибудь из личной охраны или в компании вообще имеется только один сотрудник, отвечающий за “всю безопасность”*, то здесь даже речи не может быть о попытках сделать из него полноценного специалиста в области ТЗИ, который *“умеет всё”*.

В то же время, этот человек должен иметь общее представление и “ориентироваться” в вопросах ТЗИ, а так же уметь осуществлять мероприятия, для которых не требуется какая-либо специальная техника – *в частности, проведение визуального осмотра*.

Небольшое заключение – *для “начинающих работников” в области ТЗИ*.

Во-вторых, никогда нельзя “расслабляться” и думать, что ты стал “самым крутым” – даже, если у тебя появился некоторый опыт работы и ты чему-то научился.

Понятно, что каждый из нас считает себя **умнее других** – *иногда, так оно и есть*. Но считать себя **умнее всех** *(т.е. “**самым умным**”)* и быть уверенным, что теперь ты такой *“крутой штуцер”*, что тебя никто не сможет *“сделать”* – это неправильно. Если же ты действительно начинаешь считаешь себя “**умнее всех**” – *я сейчас имею ввиду не “по жизни” в целом, а именно в профессиональном плане* – то можно с высокой долей уверенности сказать, что ты “умер” как специалист.

Я это к тому, что **нельзя недооценивать “вероятного противника”** и нельзя делать свою работу *(в частности, специальную проверку или специальное обследование)* кое-как *“на расслабоне”*, думая, что ты *“всё знаешь и умеешь”*.

Как уже было сказано, окончание каких-либо курсов или даже ВУЗа по профилю ТЗИ – это очень хорошо, но это только “азы”, которые необходимо знать “по определению”, если ты настроен **реально** заниматься этим делом.

Образно говоря, первичная подготовка *(базовое образование)* по ТЗИ – это “штамповка”, в результате которой “что-то формируется”, а далее необходима “шлифовка”, которая длится не один месяц – *для настоящего специалиста она продолжается постоянно*.

И постоянно помнить, что “**опыт** работы” и *“стаж работы”* – это абсолютно разные вещи:

“Было бы понятие в голове. Вот ты у меня десять лет в оркестре играешь, а не можешь отличить гопака от похоронного марша.”

*(х/ф **“Максим Перепелица”**).*

Небольшое заключение – *для “начинающих работников” в области ТЗИ*.

В-третьих, нужно чётко понимать, что кроме “технологии” проведения проверки помещения существует ещё и “тактика”.

Как говорил во время утреннего осмотра наш старшина батареи в “учебке”: ***“Можно каждый день стричься и быть нестриженным”***.

Типовой пример: если в компании есть *“засланный казачёк”*, который в рабочие дни утром устанавливает диктофон или видеорегистратор в кабинет руководителя, переговорную комнату или в другое “важное” помещение, а вечером его забирает, то никакая даже самая качественная специальная проверка, проводимая после работы или в выходные дни, не сможет обнаружить эту “закладку” – *потому что в момент проведения проверки “закладки” просто не будет в данном помещении*.
В такой ситуации, чтобы проверка помещения была реально эффективной, её надо проводить внезапно непосредственно в рабочее время.

В то же время, как было сказано ранее, для проведения качественной проверки “полноценного” помещения – *в котором имеется мебель, бытовая техника, различные предметы интерьера, книги и т.д*. – потребуется длительное время и её не получится проводить “ежедневно в течении получаса” *(как физзарядку)*.

Поэтому необходимо чётко представлять все возможные угрозы, реально актуальные для конкретного объекта, – *ещё раз повторю про разработку **модели нарушителя**, которая является основой для организации работ по защите информации* – и правильно выбирать время, “глубину” и периодичность проведения проверок.

Ещё раз о техническом оснащении “поисковика”.

Ещё раз хочу сказать несколько слов по поводу оснащения поисковой техникой, когда речь идёт о “своём” подразделении защиты информации.

Моё личное мнение, которое было уже сказано ранее: техника “вторична” и её нужно приобретать только после того, когда в компании будет более-менее подготовленный толковый сотрудник *(ключевое слово “**толковый**”)*, который сможет её освоить и в дальнейшем реально **грамотно с ней работать**.

Бесполезно что-то покупать *(даже когда есть деньги на приобретение)*, если потом эта техника будет лежать *“мёртвым грузом”* где-то на складе или её дадут какому-то *“дятлу”*, который вообще ничего не понимает и который будет *“заколачивать гвозди микроскопом”, имитируя “бурную деятельность”*.

Что касается конкретного набора поисковой техники, то хочу обратить внимание на типовую ситуацию, характерную для абсолютного большинства молдавских компаний: когда отдельного подразделения, занимающегося защитой информации, в компании нет, а этим вопросом занимается “по совместительству” кто-то из *“лички”*.

В этом случае, как было сказано ранее *(моё личное мнение)*, основное внимание при проведении поисковых работ должно быть уделено визуальному осмотру помещения с помощью тех технических средств, которыми *может эффективно работать толковый сотрудник, не имеющий специального технического образования*.

Кроме того, нужно помнить о реальном уровне финансирования – как было сказано, в большинстве случаев максимальная сумма выделенных средств 2000 – 3000 USD.

Ещё раз о техническом оснащении “поисковика” – *моё личное мнение*.

Перечень технических средств, которые может позволить себе любая компания, готовая выделить на эти цели порядка 2000 – 3000 USD, включает в себя: **набор досмотровых зеркал** *(важны надёжность конструкции и удобство работы)*, хороший **оптический обнаружитель видеокамер** *(например, “Оптик-2”)* и хороший **портативный металлодетектор** *(например, GARRETT THD)*.
Если позволяет финансирование, то очень полезен будет ещё и **эндоскоп**.

Естественно, что на первом месте остаются три “основных поисковых инструмента”: **фонарь, отвёртка** и **лестница-стремянка** – они **обязательны в любом случае**.

Конечно же, другое оборудование тоже может быть использовано, но только в том случае, когда “поисковик” чётко знает его **реальные** возможности и реально умеет с ним работать – ещё раз повторю, что сейчас речь идёт не о *“компаниях, в которых всё по-взрослому”*, а о варианте когда *“Одному сотруднику поставили задачу – ищи! Что искать – сами пока не знают”*.

Одно дело, когда в компании уже есть какое-то оборудование – *как правило, “оставшееся по наследству” с прошлых лет (например, детектор поля и т.п.)* – в этом случае “сотрудник-поисковик” может спокойно изучать его *(начиная с очень внимательного чтения инструкции)* и спокойно “тренироваться” работать с ним, а потом сделать вывод о его эффективности и целесообразности использования.
И совсем другое дело, когда “возникает идея” о покупке “чего-то” – *как правило, под влиянием рекламы* – при этом очень высока вероятность *“купить кота в мешке”*.

Пример “минимального” набора.

Ещё раз о необходимости “комплексного подхода” к вопросам ТЗИ.

Ещё один важный момент, который должны чётко понимать и постоянно помнить как *“заказчики” (“работодатели”)*, так и *“исполнители” (“работники”)*: защита информации – это целый комплекс мероприятий и нельзя **“зацикливаться”** только на **“проверках помещения”**.

Если у вас на объекте *бардак* и *“проходной двор”*, то вообще нет смысла тратить время и деньги на проведение *“каких-то проверок”* – от этого не будет никакого толку.

Как было уже несколько раз сказано ранее, есть ещё две “составляющие”, которые *(на мой взгляд)* более важны и эффективны для защиты информации: **организационно-режимные** и **технические мероприятия**.

Правильно организованные и **реально выполняемые** на объекте **организационно-режимные мероприятия** смогут “отсечь” большинство угроз, связанных с возможной утечкой информации из “защищаемых” помещений – в первую очередь речь идёт о предупреждении установки *(“заноса”)* средств съёма информации в данные помещения.

А **правильный выбор** и **грамотное использование технических средств защиты информации** позволят “заблокировать” *(“закрыть”)* некоторые возможные каналы утечки информации и максимально снизить эффективность работы некоторых возможно внедрённых средств съёма информации.

Ещё раз о необходимости “комплексного подхода” к вопросам ТЗИ.

В “идеальном варианте” для защиты информации на объекте должны быть совместно реализованы все три вида мероприятий: **организационно-режимные**, **технические** и **поисковые** – *при этом они должны “дополнять” и “страховать” друг-друга*.

Нужно чётко понимать, что организационно-режимные и технические мероприятия по защите информации – это серьёзная работа, а их грамотная разработка и правильная реализация возможны только опытными специалистами.

Безусловно, есть “базовые” мероприятия, которые актуальны не только для защиты информации, но и для решения более общих задач, связанных с охраной объекта – в частности, речь идёт о системе охранно-пожарной сигнализации, системе охранного видеонаблюдения и об организации доступа на объект.
Но есть целый ряд “специфических” мер, которые касаются именно обеспечения защиты информации, циркулирующей на объекте.

Необходимо отметить, что реализация на объекте организационно-режимных и технических мероприятий по защите информации в обязательном порядке потребует тесного взаимодействия с различными подразделениями (отделами) компании.

“Полноценный” разговор об организационных и технических мероприятиях займёт очень много времени, поэтому ***в рамках данной презентации о них будет сказано буквально несколько слов****.*

Немного об организационно-режимных мероприятиях.

Что касается **организационных мероприятий**, то они не требуют применения какой-либо специальной техники. Образно говоря, это ряд правил, которые при их правильном выполнении позволяют существенно ограничить возможности злоумышленника по доступу к интересующей его информации.

В частности, нужно чётко понимать, что “закладка” не может “сама попасть” в помещение – её туда должен кто-то принести *(обычно “целенаправленно”, но в ряде случаев человека могут использовать и “втёмную”, когда он сам даже не подозревает об этом)*. Для предупреждения *(максимального уменьшения)* вероятности такого “попадания” существует целый ряд мер, которые могут быть реализованы в любой компании. Естественно, что “компания компании рознь” и уровень предлагаемых организационно-режимных мероприятий должен соответствовать “уровню” конкретной компании.

Но тут есть один принципиальный момент – *на сколько руководство компании готово к тому, чтобы эти правила **реально** выполнялись сотрудниками компании и, в первую очередь, **выполнялись самим руководством***.

Типовой пример: ограничение на наличие средств мобильной связи и других электронных устройств, имеющих “штатный” микрофон и камеру *(“планшеты”, ноутбуки и т.п.)*, при проведении конфиденциальных мероприятий – обычно *“на бумаге”* всё выглядит очень *“красиво”* и *“строго”*, но в реальности в большинстве случаев этот запрет постоянно нарушается *(причём самими руководителями компаний)* и, как правило, его просто “не воспринимают всерьёз”.

Немного об организационно-режимных мероприятиях.

Необходимо отметить, что существует целый ряд “типовых” мероприятий, которые важны и эффективны: *организация пропускного режима на объект и разграничение доступа в помещения на самом объекте;*
проведение так называемого “категорирования помещений”;
разработка процедуры приобретения и установки предметов интерьера в важных помещениях (в том числе речь идёт и о бытовой электронике);
организация видеоконтроля за важными помещениями и т.д.

Все эти мероприятия прежде всего предназначены для серьёзных компаний, в которых “всё по-взрослому” – т.е. в них есть штатное подразделение по защите информации, которое реально работает и взаимодействует с объектовой охраной, подразделением IT, отделом кадров, хозяйственным отделом и т.д.

При этом следует постоянно помнить об **элементарных вещах**, которые не требуют каких-либо затрат или специальных навыков и которые “по определению” должны выполняться любым здравомыслящим человеком:
*не вести конфиденциальные разговоры в каких-нибудь “левых” местах, в помещениях с открытыми окнами или не закрытыми дверьми – да и вообще поменьше болтать (как говорится: “**Не знаешь – молчи, знаешь – помалкивай**”);*
не оставлять своё помещение без контроля и при выходе закрывать его;
не “светиться” в окнах – они должны быть закрыты шторами или жалюзи.

Вроде бы элементарные простые вещи, а сколько от них пользы.

Немного о технических мероприятиях по защите информации.

Что касается **технических мероприятий** по защите информации, то это мероприятия, предусматривающие применение специально разработанных технических средств защиты информации, а также реализацию технических решений.

Необходимо отметить, что **реально** заниматься данным вопросом может только человек, имеющий базовое техническое образование и необходимую подготовку в области ТЗИ. Это связано с тем, что при проведении технических мероприятий по защите информации нужно знать и понимать ещё больше “технических вещей”, чем при проведении специальных проверок – *моё личное мнение*.

В то же время, абсолютное большинство *“технических решений”* (кавычки!), предлагаемых *так называемыми “специалистами”*, являются “имитацией” – причём очень часто не столько из-за желания *“развести”* заказчика *(это само собой)*, сколько из-за полной некомпетенции этих *“специалистов”*.

Чего только стоит *“типовая рекомендация”* таких *“специалистов”*, которые в качестве *“средства защиты”* предлагают своим “заказчикам” приобрести у них *“глушилку GSM”*, которая якобы *“полностью защитит от любой прослушки”*.

Речь даже не о том, что блокиратор GSM абсолютно бесполезен для борьбы с диктофонами, проводными микрофонами, радиомикрофонами и видеокамерами.

В ряде случаев блокирование даже “обычного” GSM-передатчика будет практически невозможно с помощью такой *“глушилки” – например, если “базовая станция” сотовой связи находится в непосредственной близости от места использования “блокиратора”, то эффективность его работы будет практически “нулевой” (зависит от его типа)*.

Немного о технических мероприятиях по защите информации.

Аналогичная ситуация с использованием генераторов электромагнитного шума, средств вибро-акустической защиты, “ультразвуковых” подавителей, специальных фильтров и т.д. – *там очень много нюансов, которые может знать только реальный специалист*.

Нужно чётко понимать, что различные технические средства защиты информации предназначены для “борьбы” только с конкретными видами угроз – *причём эта “борьба” идёт с большей или меньшей эффективностью*.

Как было сказано ранее: *“чудо-коробочки с красной кнопкой”* – не существует.

Поэтому задача **настоящего** специалиста состоит в том, чтобы разработать и реализовать оптимальное для конкретного объекта комплексное решение по защите информации, в котором будут задействованы в том числе и необходимые технические мероприятия.

Естественно, что эффективное и грамотное решение может предложить только настоящий специалист в области ТЗИ, а не различные “шаромыжники”, торгующие непонятными *“глушилками”* и *“шумелками”*.

Как говорил в “**Двенадцати стульях**” заведующий Старкомхозом тов. Гаврилин: *“Трамвай построить – это не ешака купить”*.

Так что ещё раз повторю: для того, чтобы грамотно разработать и реализовать технические мероприятия по защите информации, **требуется принципиально более глубокая подготовка сотрудника**, чем для проведения поисковых работ.

Немного о “взаимоотношении” между *“работником” и “работодателем”*.

Хочется обратить внимание на момент, касающийся профессиональных взаимоотношений между сотрудником и “работодателем” (владельцем компании).

На мой взгляд, на вопрос *“Что хуже: начальник-дурак или работник-дурак?”* нельзя ответить однозначно – всё зависит от конкретной ситуации.

Многие бизнесмены имеют “своё представление” по вопросам защиты информации. Очень часто это “представление” является *“фильмово-фантастическим”* и они уверены в существовании *“чудо-аппаратов, которые всё найдут”* и *“чудо-коробочек с красной кнопкой, которые от всего защитят”*.

Очень хорошо если руководитель компании адекватный человек, который не считает себя *“всезнающим пророком”* – ему можно спокойно всё объяснить и он поймёт. В этом случае главное, чтобы “дураком” не оказался уже “работник”, который может так “загрузить” своего “шефа” всякой хе**ёй, что будь здоров…

Совсем другое дело если “работодатель” (владелец компании) считает себя *“самым умным”* и уверен, что только он знает всё – в том числе и в тех областях, о которых у него нет ни малейшего профессионального представления. Такой “работодатель” точно будет требовать, чтобы ему любой ценой достали *“чудо-коробочку с красной кнопкой”*, которую он видел в “шпионском” фильме. В этом случае сотруднику, отвечающему за защиту информации, можно только посочувствовать и напомнить ему старую восточную пословицу: *“Будешь спорить с царём – погубишь себя, будешь с ним во всём соглашаться – погубишь царя”*.

Заключение.

Угроза утечки информации или её съёма с использованием специальных технических средств в ряде случаев является достаточно реальной проблемой как для различных коммерческих структур, так и для отдельных граждан.

Понятно, что в каждом конкретном случае всё “очень индивидуально”.
Так, например, я абсолютно согласен с очень хорошей фразой с форума на сайте www.analitika.info, которая касается “классического” промышленного шпионажа: *“Если для конторы двенадцать штук зелени в год – проблема, то у неё нечего тырить. Особенно с использованием технических средств”*.
В то же время, в раздевалке любого спортивного комплекса или в обычной квартире может находиться устройство, предназначенное для скрытой видеозаписи, которое установил какой-нибудь *“озабоченный” долб**б*.
Поэтому тут, как говорится, *“не угадаешь”* – хотя всегда надо не *“гадать”*, а думать.

Нужно чётко понимать, что защита информации в целом и поиск устройств съёма информации в частности – это серьёзная и многосторонняя работа, которую реально может выполнить только настоящий специалист *(таких очень мало)*.
А вариант: *“Пришёл. Увидел. Победил.”* – здесь не проходит.
Здесь нужно **думать**, **учиться** и “**мудохаться**” *(в хорошем смысле этого слова)*.

Надеюсь, что данная презентация помогла тем, кто верил в существование *“чудо-приборов”*, *“чудо-коробочек с красной кнопкой”* и *“чудо-специалистов”*, реально взглянуть на ситуацию и понять, что никаких *“чудес”* здесь не существует.

Несколько финальных слов о моей презентации.

Как было сказано в самом начале, данная презентация отражает моё личное мнение, *в котором я убеждён, исходя из своего скромного опыта работы в области технической защиты информации*.

В то же время, **вполне возможно, что моё мнение – ошибочное**, а я не только абсолютно не компетентен в данном вопросе, но и вообще “тормоз” *(как говорится, у каждого своя правда)*.

Поэтому всё, что я “изложил” в презентации, **должно оцениваться слушателями критически** и **обязательно должно быть проверено ими как из других источников**, **так и на своём собственном опыте** – *в ходе практической работы*.

Ещё раз повторю, что данную презентацию нельзя рассматривать в качестве какого-то “полноценного учебного пособия” – её основной целью было **не “научить”** *(как я сказал, это вообще не реально в рамках “самиздата”)*, а именно **познакомить** с основами *(“базовыми” моментами)* и попытаться **сформировать** у слушателей **общее представление** по данному вопросу.

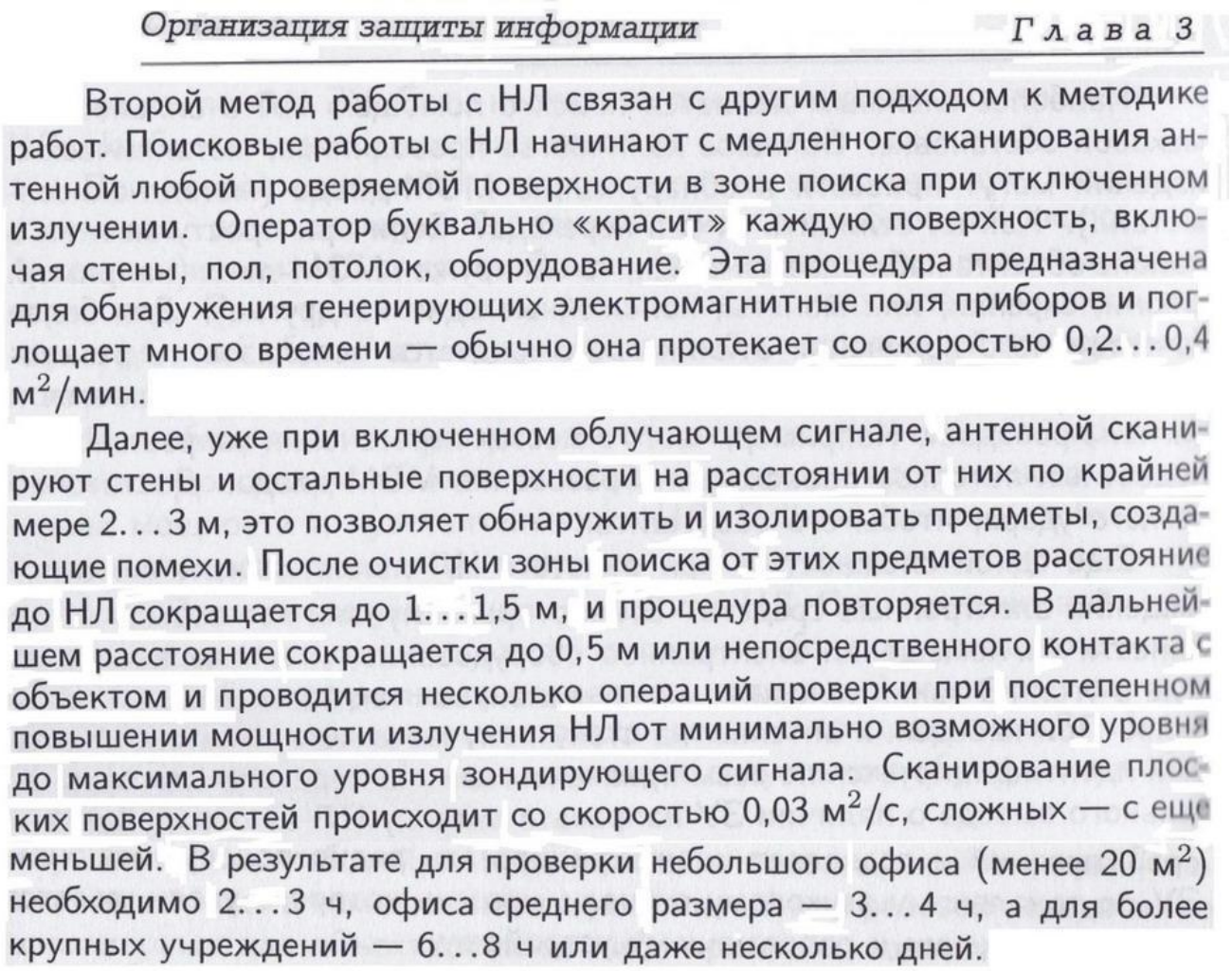
Если же кто-то из слушателей захочет “копать глубже” и заниматься вопросами технической защиты информации серьёзно, тогда ему необходимо как минимум получить более-менее полноценное “начальное” образование в данной области.

Для адекватных думающих людей, имеющих базовое техническое образование, возможен вариант самостоятельного обучения – *при наличии соответствующих учебных пособий (материалов) и возможности практической работы*.

Не всё, что пишут и говорят – “истина в конечной инстанции”.

В открытом доступе имеется достаточно большое количество различных *“пособий”* по вопросам ТЗИ.
В то же время, любую информацию нужно “оценивать критически” и если вас в ней что-то “смущает”, то надо разбираться, а **не воспринимать** её как *“абсолютную истину”*.

Например, вот такая *“оригинальная методика”* работы с нелинейным локатором *(см. фото)*.



Организация защиты информации *Глава 3*

Второй метод работы с НЛ связан с другим подходом к методике работ. Поисковые работы с НЛ начинают с медленного сканирования антенной любой проверяемой поверхности в зоне поиска при отключенном излучении. Оператор буквально «красит» каждую поверхность, включая стены, пол, потолок, оборудование. Эта процедура предназначена для обнаружения генерирующих электромагнитные поля приборов и поглощает много времени — обычно она протекает со скоростью 0,2...0,4 $м^2$/мин.

Далее, уже при включенном облучающем сигнале, антенной сканируют стены и остальные поверхности на расстоянии от них по крайней мере 2...3 м, это позволяет обнаружить и изолировать предметы, создающие помехи. После очистки зоны поиска от этих предметов расстояние до НЛ сокращается до 1...1,5 м, и процедура повторяется. В дальнейшем расстояние сокращается до 0,5 м или непосредственного контакта с объектом и проводится несколько операций проверки при постепенном повышении мощности излучения НЛ от минимально возможного уровня до максимального уровня зондирующего сигнала. Сканирование плоских поверхностей происходит со скоростью 0,03 $м^2$/с, сложных — с еще меньшей. В результате для проверки небольшого офиса (менее 20 $м^2$) необходимо 2...3 ч, офиса среднего размера — 3...4 ч, а для более крупных учреждений — 6...8 ч или даже несколько дней.

Я думаю, что скорее всего это некорректный перевод статьи, в которой речь шла не о “методе работы с НЛ”, а об “оценке чистоты спектра” на частотах 2-ой и 3-ей гармоники.
А ведь возможно, что кто-то, прочитав эту “методику”, пытался по ней работать…

Пример фундаментального – *звучит очень “громко”, но на мой взгляд именно так и есть* – учебного пособия по технической защите информации.

Хорев А.А. Способы и средства зашиты информации. – М.: МО РФ, 2000. – 316 с.

В учебном пособии на основе открытых публикаций отечественной и зарубежной литературы даются классификация и описание методов и средств защиты информации от утечки по техническим кангалам при ее обработке техническими средствами, а также методов и средств защиты акустической (речевой) информации. Особое внимание уделено анализу технических характеристик и способов применения средств поиска электронных устройств перехвата. Коротко рассмотрены вопросы лицензирования деятельности в области защиты информации, сертификации средств защиты информации, а также аттестования объектов информатики и организации защиты информации на объектах ТСПИ.

Для руководителей и специалистов подразделений по защите информации.

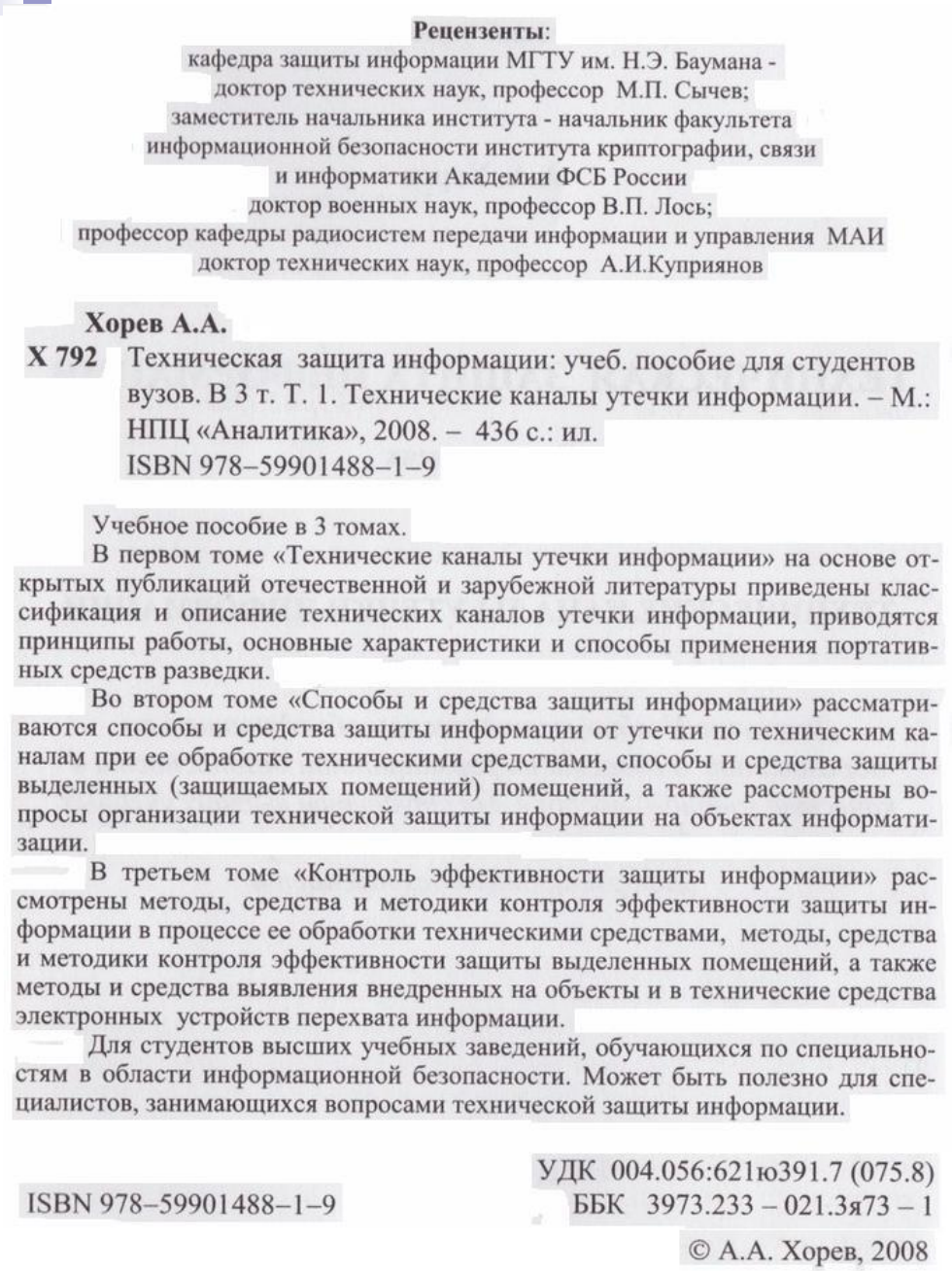
Ил. 89, табл. 39, библ. 164 назв.

Данная книга была издана более 20 лет назад, но (на мой взгляд) до сих пор является одним из наиболее фундаментальных и системных учебных пособий по технической защите информации.

ОГЛАВЛЕНИЕ

Пример фундаментального учебного пособия по ТЗИ.

Насколько мне известно, данное учебное пособие было переработано автором и существенно дополнено.
Но, к большому сожалению, переиздание данной книги, планировавшееся в виде трёхтомного учебного пособия,
так и не было завершено –
в 2008 году был издан только первый том, посвящённый техническим каналам утечки информации.



Рецензенты:
кафедра защиты информации МГТУ им. Н.Э. Баумана -
доктор технических наук, профессор М.П. Сычев;
заместитель начальника института - начальник факультета
информационной безопасности института криптографии, связи
и информатики Академии ФСБ России
доктор военных наук, профессор В.П. Лось;
профессор кафедры радиосистем передачи информации и управления МАИ
доктор технических наук, профессор А.И.Куприянов

Хорев А.А.
Х 792 Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.: ил.
ISBN 978–59901488–1–9

Учебное пособие в 3 томах.
В первом томе «Технические каналы утечки информации» на основе открытых публикаций отечественной и зарубежной литературы приведены классификация и описание технических каналов утечки информации, приводятся принципы работы, основные характеристики и способы применения портативных средств разведки.
Во втором томе «Способы и средства защиты информации» рассматриваются способы и средства защиты информации от утечки по техническим каналам при ее обработке техническими средствами, способы и средства защиты выделенных (защищаемых помещений) помещений, а также рассмотрены вопросы организации технической защиты информации на объектах информатизации.
В третьем томе «Контроль эффективности защиты информации» рассмотрены методы, средства и методики контроля эффективности защиты информации в процессе ее обработки техническими средствами, методы, средства и методики контроля эффективности защиты выделенных помещений, а также методы и средства выявления внедренных на объекты и в технические средства электронных устройств перехвата информации.
Для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности. Может быть полезно для специалистов, занимающихся вопросами технической защиты информации.

ISBN 978–59901488–1–9
УДК 004.056:621ю391.7 (075.8)
ББК 3973.233 – 021.3я73 – 1

На фото слева “общая информация” о планировавшемся к изданию трёхтомном учебном пособии “**Техническая защита информации**” (автор **А.А.Хорев**).

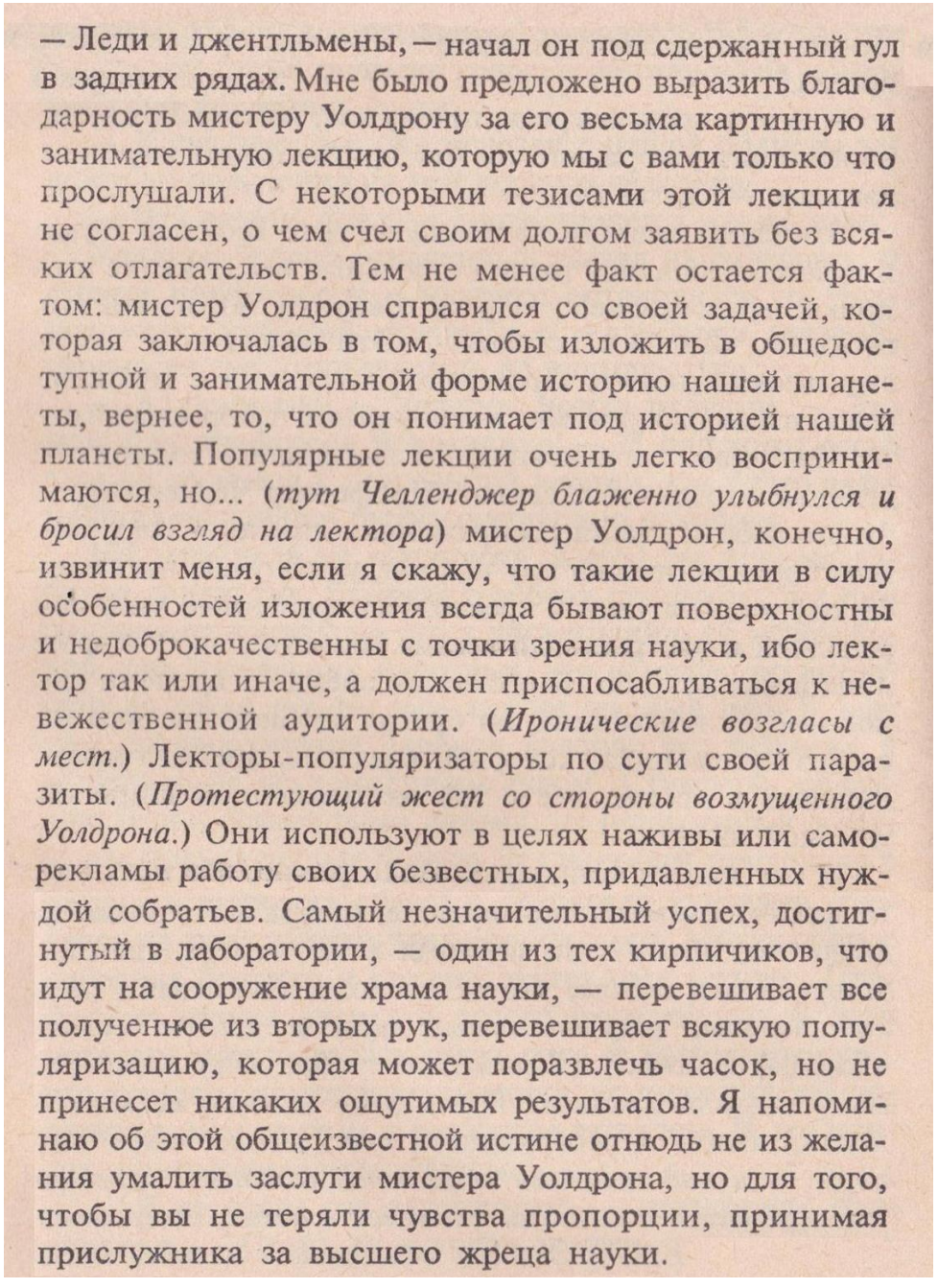
Как было сказано, к сожалению, был издан только первый том: “Технические каналы утечки информации”. Думаю, что те, кому удалось в своё время приобрести эту книгу, оценили её по достоинству.

Немного “самокритики”.

Как я говорил в самом начале, данной презентацией я постарался “обозначить проблему” *(как я её вижу)* и попытался “подтолкнуть” слушателей задуматься над этой проблемой.

А учитывая тот факт, что данная презентация предназначена для людей, не имеющих какой-либо подготовки в области защиты информации, то она была сделана в *общедоступной* и *“популярной”* форме изложения. Поэтому я считаю, что в её отношении абсолютно правильны слова *профессора Челленджера из **“Затерянного мира”** Артура Конан Дойля (см. фото)*.

Правда, я не считаю себя *“паразитом”*, так как не ставил своей целью ни *“наживу”*, ни *“саморекламу”*, ни *“поразвлечь часок”* – *скорее, всё было совсем наоборот*.



— Леди и джентльмены, — начал он под сдержанный гул в задних рядах. Мне было предложено выразить благодарность мистеру Уолдрону за его весьма картинную и занимательную лекцию, которую мы с вами только что прослушали. С некоторыми тезисами этой лекции я не согласен, о чем счел своим долгом заявить без всяких отлагательств. Тем не менее факт остается фактом: мистер Уолдрон справился со своей задачей, которая заключалась в том, чтобы изложить в общедоступной и занимательной форме историю нашей планеты, вернее, то, что он понимает под историей нашей планеты. Популярные лекции очень легко воспринимаются, но... (*тут Челленджер блаженно улыбнулся и бросил взгляд на лектора*) мистер Уолдрон, конечно, извинит меня, если я скажу, что такие лекции в силу особенностей изложения всегда бывают поверхностны и недоброкачественны с точки зрения науки, ибо лектор так или иначе, а должен приспосабливаться к невежественной аудитории. (*Иронические возгласы с мест.*) Лекторы-популяризаторы по сути своей паразиты. (*Протестующий жест со стороны возмущенного Уолдрона.*) Они используют в целях наживы или саморекламы работу своих безвестных, придавленных нуждой собратьев. Самый незначительный успех, достигнутый в лаборатории, — один из тех кирпичиков, что идут на сооружение храма науки, — перевешивает все полученное из вторых рук, перевешивает всякую популяризацию, которая может поразвлечь часок, но не принесет никаких ощутимых результатов. Я напоминаю об этой общеизвестной истине отнюдь не из желания умалить заслуги мистера Уолдрона, но для того, чтобы вы не теряли чувства пропорции, принимая прислужника за высшего жреца науки.

Основной итог.

В завершении ещё раз хочу повторить **основную идею**, которую я попытался довести этой презентацией как до “заказчиков” *(“работодателей”)*, так и до “исполнителей” *(“работников”)*:

В вопросах, касающихся защиты информации в целом и поиска устройств съёма информации в частности *(как и в любом другом деле)*, **нужно прежде всего ДУМАТЬ**.

Причём **думать своей головой**, а *не мобильным телефоном, не “Google”, не “Яндексом” и т.п*.

И помнить очень хорошую фразу: ***Знание человеческое ограничено, а глупость человеческая – бесконечна***.

Так что успехов!