новости

ГЛАВНАЯ

ФОТО И ВИДЕО

НОВОЕ НА САЙТЕ •••

Военное обозрение
Вооружение
Технологии

МНЕНИЯ

АНАЛИТИКА

«Голый король»

23 декабря 2013

Нынешняя ситуация с информационной безопасностью в России, если посмотреть на нее непредвзято, полностью соответствует сюжету известной детской сказки «Голый король».

вооружение история

Плачевность ситуации, государственная власть, в лице первых лиц, начала понимать только после сливов секретной информации небезызвестным Сноуденом, он, является тем мальчиком, который указал пальчиком на очевидное.

И произнес сакральные слова, которые, наконец-то услышали руководители страны.

Что творится сейчас в профильных государственных структурах, профессионалы знают. Как всегда у нас, кампанейщина доходит до маразма, но «трясут» круто, грозят оргвыводами и посадками.

Больше ничего говорить на глобальные темы не буду, а то меня «понесет», как незабвенного Остапа. Перейду к конкретному примеру, надеюсь всем, даже не профессионалам, все станет очевидным.

Бизнес по-русски

Как-то на досуге наткнулся на статью в Комсомольской правде «В Россию поставляют ноутбуки-шпионы?», речь в ней шла о защищенном ноутбуке Getac A790 Тайваньской компании Getac Technology.

Вот этот «красавец»:



В статье говорилось о наличии на этом компьютере предустановленной программы Computrace LoJack, разработанной канадской фирмой Absolute Software. Утверждалось, что программа приходит в активированном виде и сразу пытается подключиться к серверам в Канаде. Кроме того фирма производитель стимулировала продавцов техники в России для предоставления ей форвардной информации о заказчиках данных защищенных компьютеров.

утверждалось, что данные компьютеры широко применяются в Российских вооруженных силах....

Прочитав статью в «Комсомолке» сразу вспомнил о материале трехлетней давности

Заинтересовавшись зашел на сайт разработчика программы и читаю, действительно,-

Программная часть системы Computrace LoJack, состоит из двух модулей, первый

В заключении делался однозначный вывод о целевой акции потенциального противника и

посвященной этой же программе на сайте rom.by: «BIOS-ный троян от Absolute Software». Там подробно описывался механизм размещения и работы в БИОС программного модуля этой программы, так что тема не нова.

программа посылает данные геолокации на удаленный сервер, имеет возможности удаленной блокировки компьютера и стирания информации с дисков по командам с серверов фирмы Absolute Software. Кроме этого возможен полный цикл удаленного менеджмента ноутбука начиная от обновления БИОС, установки, удаления любых программ и кончая переустановкой ОС. Официальное предназначение программы - предотвращение утечки данных и использования ноутбука в случае его кражи или потери.

прописывается в БИОС на этапе производства компьютера, а второй подгружается из сети в случае, если владелец компьютера решает воспользоваться программой Computrace LoJack. Причем этот сервис не бесплатен, нужно платить порядка \$50 за годовую подписку на услуги фирмы Absolute Software.

Альтруизм не свойственен бизнесу, бесплатная активация платного сервиса говорит о том, что получаемая от этого выгода оправдывает финансовые затраты (бесплатно не значит «даром»). Кто платит за информацию думаю тоже понятно...

Взглянув на изображение защищенного ноутбука Getac A790 сразу вспомнил про виденный на площадке одного из заказчиков аналогичный серый ящик, он был задвинут в угол, весь в пыли, и похоже давно не использовался. Захотелось «пощупать» машинку самому и в следующий приход к этому заказчику сразу направился к заинтересовавшему меня пыльному ящику.

Открываю и не веру своим глазам, это не ноутбук Getac A790, судя по шильдику на лицевой панели, это Российский компьютер МВК-2, более того, на этикетке все данные о модели и производителе, где написано, что это изделие произведено фирмой «ИнфоПро» в 2010году. Кроме этого на ноутбуке красуется голографический стикер спецпроверки.

Для незнающих поясню, спецпроверка и специсследования это необходимые процедуры (и

очень дорогостоящие) для того, чтобы техника появилась на секретных объектах и в войсках. После этих проверок техника считается безопасной с точки зрения утечек секретной и конфиденциальной информации и может использоваться на секретных и защищенных объектах. Ящик заинтриговал и не включить его я просто не смог, руки сами потянулись к клавиатуре,

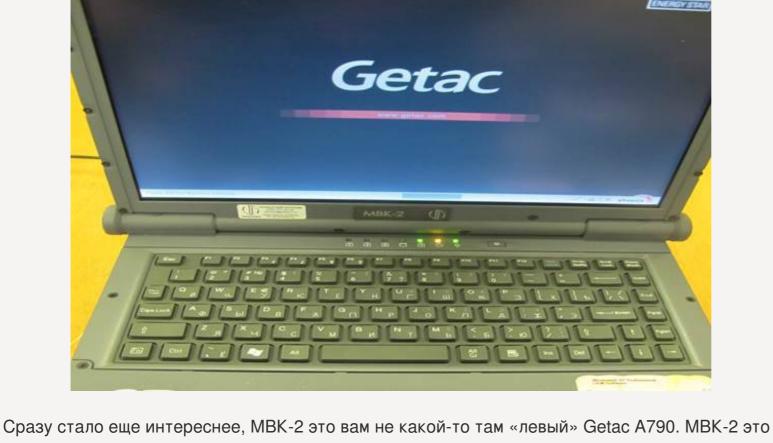
включаю, на экране появляется заставка инициализации и сразу все становится на свои

и на российском компьютере MBK -2 гордо высвечивается название: Getac A790.

места, - классический вариант «бизнеса по русски». Российская фирма, называющая себя разработчиком и изготовителем МВК-2 (ИнфоПро), даже не удосужилась прописать в БИОС собственную графическую заставку инициализации

Я не поленился и заснял это «чудо» на мобильник, вот ОНО.

выявили наличие в МВК-2 этой официальной «закладки».



России, отечественная разработка, в войсках их тысячи, если не десятки тысяч... Ну, по поводу отечественной разработки и отечественной сборки мне стало все сразу понятно, а вот имеются ли там после специсследований и спецпроверки (о чем свидейтельствовал голографический стикер) программы фирмы Absolute Software мне было интересно. Воспользовавшись свободным временем, даже не спрашивая заказчика (каюсь,

Мобильный Вычислительный Комплекс, - основной защищенный компьютер Вооруженных Сил

грешен) просканировал БИОС на наличие сигнатуры программы Computrace LoJack, которую взял из статьи на сайте rom.by. И не удивился, когда их там обнаружил. Инженеры ИнфоПро из БИОС своих компьютеров ничего не удалили, а все специальные исследования не

Еще не сделали заказ на iHerb?

Более 35 000 полезных товаров. Низкие цены. Скидки! Доставка по России!

Бестселлеры Скидки Новинки

Пробные Товары

ru.iherb.com

Перейти

Яндекс. Директ



как в его стране относятся к русским

Самые красивые женщины в мире: Топ 10 стран

Таджик рассказал,



Вопрос шенгенских виз может изменить

позиции ЕС по



Российское эмбарго запустило цепную реакцию в Литве



В Петербурге орудует банда хитроумных кочевников. Фото



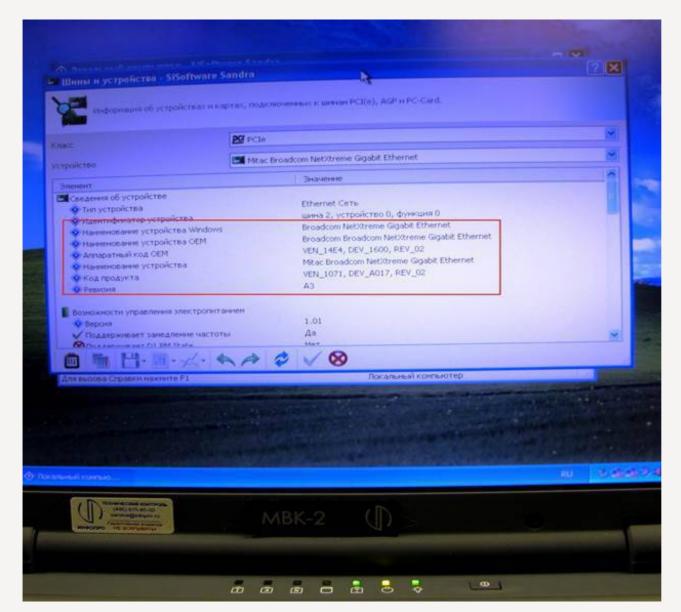
Тупизна и наглость «производителя» поражает, есть официальные программы для сборки/разборки БИОС, можно любой модуль из БИОС удалить, либо вставить без проблем, что мешало специалистам ИнфоПро вставить собственную заставку для экрана и вырезать скандальный модуль из БИОС? Эту процедуру освоили все отечественные сборщики, она не уникальна...

«Паленые» чипы

К сожалению, машина не была подключена ни к Интернету ни к локальной сети, поэтому не удалось посмотреть сетевую активность на IP адресах, чтобы выяснить в каком состоянии находится сервис фирмы Absolute Software.

Единственное, что сделал, это сфотографировал экраны диспетчера устройств в программе Sandra, чтобы на досуге разобраться с аппаратурой внутри MBK-2. Было ощущение, что \$50 баксов за активацию программы Computrace LoJack платится не просто так, в этой штуковине есть еще «чудеса».

Вот фото экрана заинтересовавшего меня конкретно:



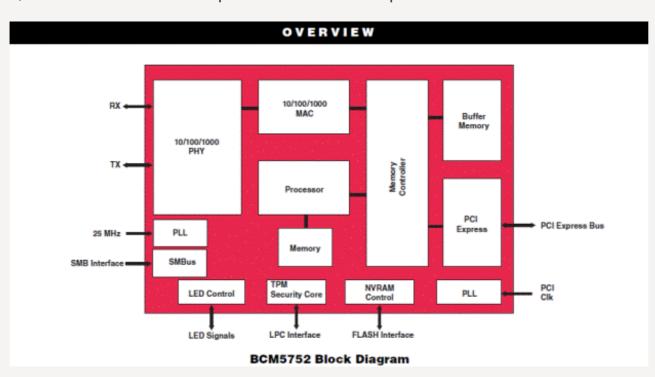
Сетевые чипы фирмы Broadcom установленные в MBK-2 давно пользуются дурной славой, как потенциальные площадки для размещения закладок. По кодам производителя вышел на конкретную микросхему Broadcom BCM 5752.

У фирмы Broadcom целая линейка чипов серии BCM 57хх. Чипы этого семейства засветились на множестве хакерских сайтов, даже наш отечественный журнал «Хакер» как минимум дважды писал в прошлом году о закладках на этих чипах.

Была статья «Руткит в сетевухе: фантазии программиста о создании непобедимого руткита» и более конкретная новость со ссылкой на успешный эксплоит: «Руткит в сетевой карте». Так что чипы BCM 57хх хакеры используют для своих целей достаточно давно, это не секрет.

В чипах серии ВСМ 57хх имеется собственная флеш-память (можно подключить и дополнительно внешнюю флеш-память на выделенном SPI интерфейсе), собственная ОП, собственный RISC процессор.

Вот официальная блок схема микросхемы ВСМ 5752 примененной в МВК-2:



Фактически это компьютер в компьютере, причем программы, прошитые внутри его флешпамяти, выполняются как на собственном встроенном RISC процессоре, так и на центральном процессоре вычислительной установки, во время инициализации системы (расширенный БИОС на периферийных контроллерах).

Согласно документации внутри микросхемы находится всего 16Кбайт флеш-памяти, но на внешнем интерфейсе можно разместить дополнительно до 8Мбайт программ и данных. Представляете сколько туда можно «напихать» всего?

В связке с программой Computrace LoJack такой сетевой чип может все, что угодно. Узнать содержимое флеш-памяти этого чипа можно только на инструментальном стенде, да и то не факт, что это получится. У меня опять начался приступ шпиономании, но уже не виртуальной, а сетевой.

Строгость законов и необязательность их исполнения

Пристально вглядываюсь в блок-схему чипа, можно сказать сверлю ее взглядом, и наконец, до меня доходит, - TPM Security Core — это же TPM модуль!, смотрю в документацию и точно, именно в чипе BCM 5752 из этого семейства имеется встроенный TPM модуль стандарта 1.2, подключенный к LPC интерфейсу.

Наличие TPM модуля в Российском защищенном компьютере это нонсенс, законодательно запрещено даже ввозить технику с такими модулями, а использование их в военной технике, это вообще подсудное дело. Единственный вариант, чип может присутствовать на плате, но должен быть физически отключен на этапе производства и быть в неработоспособном (обесточенном) состоянии.

Формально запрет основан на использовании в этих ТРМ модулях криптографических алгоритмов зарубежной разработки. Истинная же причина запрета, в том, что ТРМ модули это средство генерации и хранения ключей шифрования и паролей имеющих в корне цепочки доверия уникальный для каждого чипа ключ (PRIVEK), который является корневым ключом шифрования по RSA алгоритму (его секретной частью).

Этот ключ знают производители чипа, и по идее никто более. Но все производители криптосредств в обязательном порядке имеют контакты со спец-службами, думаю не нужно объяснять у кого будут храниться дубликаты этих ключей?

Знание корневого ключа для конкретного TPM модуля позволяет расшифровать содержимое памяти TPM модуля и кроме того, всегда точно локализовать место конкретной вычислительной установки в сетевом пространстве.

Захотелось проверить наличие активности ТРМ модуля на МВК-2, сделать это просто, для этого есть две возможности. В системных ASPI таблицах есть специальный объект, описывающий наличие ТРМ модуля, но это только отметка в памяти. Устройство может присутствовать, а записи в таблицах о его наличии может и не быть.

Так что этот метод недостаточно надежен, если записей в системных таблицах нет, ОС его тоже не увидит.

Второй способ гораздо надежнее, любое устройство взаимодействует с остальными компонентами вычислительной системы через регистры, если эти регистры активны (их можно читать и в них писать информацию) то устройство работоспособно. По идее отключенный в условиях производства ТРМ модуль не имет работоспособных регистров. Проверить это просто, все регистры ТРМ модуля стандарта 1.2 находятся на системной шине в фиксированном адресном пространстве 0FED4_0000h - 0FED4_FFFFh, это не я придумал, так написано в стандарте.

так написано в стандарте.

Снова включая исследуемый MBK-2 я уже имел под рукой программу для просмотра регистров на системной шине (собственного производства естественно), и совсем не

Что получается если не исполнять законы

удивился обнаружив активность ТРМ модуля.

Ожидаемый результат подтвердился, регистры TPM модуля были в рабочем состоянии, соответственно чип TPM модуля никто не отключал. Только вот информация в регистрах не соответствовала спецификации. В одном из активных регистров обнаружились Скан-Коды нажатий клавиатуры...

нажатий клавиатуры...
Было похоже, что информация о скан-коде последней нажатой клавиши запоминается в

называется аппаратная закладка,- кейлоггер.

Возможно ли такое, - вполне, поскольку контроллер клавиатуры и ТРМ модуль расположены на одном интерфейсе – LPC и этот интерфейс выполнен по схеме последовательного соединения всех устройств подключенных к нему. Фактически ТРМ модуль был превращен в

регистрах ТРМ модуля, а это уже напоминало то, что на профессиональном языке

сниффер, слушающий шину и запоминающий в своих регистрах информацию с клавиатуры. Таким образом, хакерские технологии, уже более года обсуждаемые на профессиональных форумах, теперь образно говоря, на службе какой-то спецслужбы.

Аппаратный кейлоггер в MBK-2 это «круто», могу ли я ошибаться, - конечно, поскольку это предварительный результат внешнего исследования. Если бы удалось залезть внутрь этой машинки, то можно это либо доказать, либо опровергнуть, в любом случае нужно

разбираться, но у меня такой возможности нет.

Закономерный вопрос, а может кто уже разбирался и пришел к заключению что все нормально,- работать можно?

Сомневаюсь, специалисты которые не в состоянии поменять заставку в БИОС, не знающие про закладку в БИОС программы Computrace LoJack врядли даже знают что либо о ТРМ модулях, не говоря уж о том, чтобы разбираться в их спецификациях.

Так что эта непроверенная техника продолжает поступать в Россию под гордым именем «Мобильный Вычислительный Комплекс МВК-2» и несет на своем борту и явную закладку в БИОС и аппаратный кейлоггер в сетевом чипе. А этими комплексами комплектуются очень важные объекты и изделия, вот один из примеров, скачанный из Интернет:



Подвижные узлы связи Р-849М1(М) и Р-986М Р-849М1(М) предназначен для обеспечения телефонной радиосвязи на коротких, ультракоротких волнах на стоянке и в движении автомобиля операторам авиационных средств связи. В изделии обеспечивается управление радиостанциями с основного пульта управления на базе мобильной ПЭВМ типа МВК-2, резервного пульта управления и дистанционное управление с

выносного пульта, удаленного на

расстояние до 200 м.

Государственная тайна как товар

И в заключении, все-таки не удержусь от глобальных обобщений, они печальны.

В нашей стране безопасность превратилась в товар, которым торгует, кто ни попадя. Чтобы не быть голословным, приведу конкретный скриншот сайта одного из многочисленных посредников, зарабатывающих на гостайне:



Особенно умиляет откровенность формулировок текста на сайте, типа «Возможность купить лицензию ФСБ на криптографию», она подчеркнута на скриншоте красным. И это не оговорка, это еще раз проскочила «Голая правда» о «Голом короле».

То, о чем давно уже болтают в курилках, (что сотрудники 8центра ФСБ превратили выдачу лицензий в «бизнес по русски»), нашло вот такое наглядное, независимое, публичное подтверждение.

Грустно, господа...

P.S Не подумайте только, что об этой ситуации не знает власть, отнюдь.

Уже более года тому назад, обо всем, что здесь писалось докладывалось в очень «высоких кабинетах», в частности об этом информирован вице премьер Д. Рогозин.

Результат нулевой, а вот я после этого получил проблемы, но как говорится, мир не без честных и порядочных людей, пронесло.



GEOVITA - биоразлагаемая посуда geo-vita.com

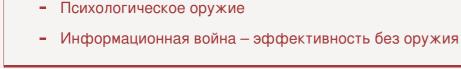
Продажа био посуды. Эко-материалы. Закажите образцы!

Яндекс.Директ

Автор: R_T_T

X





публикаций

Мнение редакции "Военного обозрения" может

не совпадать с точкой зрения авторов

Если вы заметили ошибку в тексте, выделите текст с ошибкой и нажмите

Ctrl+Enter





Аршавин в "Арсенале": от любви до ненависти Перевод материала с портала «Bleacher Report» (США)

II INOPROSPORT

Читайте также

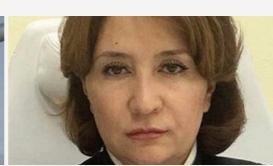
Powered by Google



СМИ Украины: мы могли растерзать «зеленых человечков»



Впечатляющий маневр: полет Cy-35 лишил дара речи американцев



Опубликовано компрометирующее фото «золотой» судьи Хахалевой



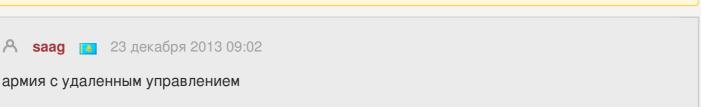
Рогозин ответил румынам за самолет: «ждите ответа, гады»

Комментарии 61



Информация

Уважаемый читатель, чтобы оставлять комментарии к публикации, необходимо **зарегистрироваться.** Уже зарегистрированы? **Войти**

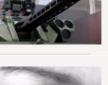




Сорик 23 декабря 2013 09:11 ↑
Какое государство, такая и армия... Уряя новые самолеты, уряя новые корабли, а потом окажется, что все это без связи и управления. Новый 41-й!



США занервничали: РФ ответила на их провокацию



любую технику противника

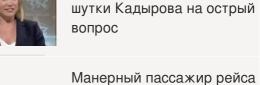
Россия ответили Польше

на «удар ниже пояса»

Госдеп негодует из-за

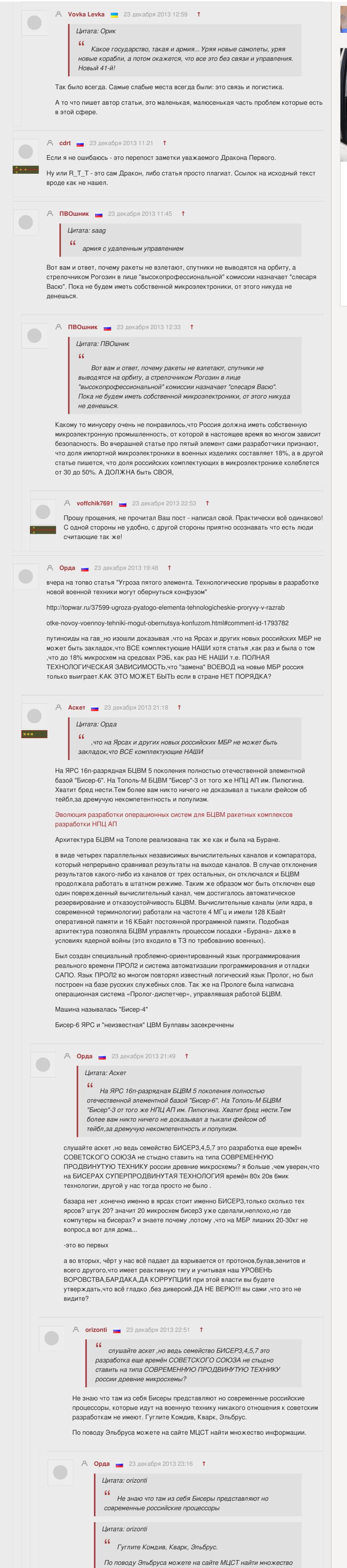
Боевой «Вихрь» уничтожит





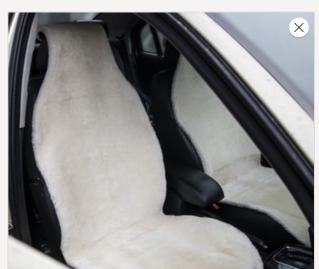
получил по лицу за

оскорбление русских



информации.





Меховые накидки для автомобиля!

100% овчина! Акция:Скидка 50% + накидки на заднее сиденье в подарок! Жмите!

2 подарка 100% овчина От производителя Оплата при получении

shop-arktika.ru Адрес и телефон

Яндекс.Директ

не знаете не говорите, где применяются эльбрусы, мцст? а вот амерские микросхемки ,как раз таки стоят в НАШИХ ВОЕННЫХ ИЗДЕЛИЯХ и это ОПАСНО для нашей ОБОРОНОСПОСОБНОСТИ. A orizonti 24 декабря 2013 01:11 1 Эльбрусы применяются в С-300 начиная с С-300ПМУ2, на различных КП и РЛС ПВО, ПРО. Комдивы применяются в бортовых авиационных системах. По крайней мере это то что достоверно известно. В общем во всех ключевых системах стоят наши процессоры. A brainkiller 24 декабря 2013 11:58 1 Цитата: Орда не знаете не говорите,где применяются эльбрусы,мцст? Эльбрус стоит на ДОН-2Н. Это лишний раз подтверждает что все новейшие Российские разработки, не такие уже новые. Какой же задел был у Советской науки?! Хорошо если Ярсы сделаны так что нашим заклятым друзьям не добраться. А вот по поводу "во вторых" совершенно согласен! Аскет 24 декабря 2013 00:20 ↑ Цитата: Орда БИСЕР3,4,5,7 это разработка еще времён СОВЕТСКОГО СОЮЗА не стыдно ставить на типа СОВРЕМЕННУЮ ПРОДВИНУТУЮ ТЕХНИКУ россии древние микросхемы? В НПЦ АП создано поколение БЦВМ семейства «Бисер». Планируется ли его продолжить? – Сейчас мы основываем наши СУ на базе БЦВМ «Бисер-6». Она является программно-совместимым продолжением хорошо зарекомендовавшей себя БЦВМ «Бисер-3». Однако у «Бисера-6» значительно улучшены габаритно-весовые, энергетические характеристики и надежность. Еще одна особенность этой машины: элементная база исключительно отечественного производства и повышенная стойкость к воздействию специальных факторов. Для парирования сбоев при воздействии специальных факторов применяются дополнительные средства функциональной защиты. Основу «Бисера-6» составляют БИС, имеющие повышенное быстродействие. СУ на базе этой БЦВМ прошла летные испытания в 2007 г. на РБ «Фрегат» регат», а также ДМ-SLБ и ДМ-03. Мы планируем использовать «Бисер-6» в СУ ракет-носителей семейства «Ангара». Кстати, СУ для «Ангары» уже в каком-то смысле отработана при пусках южнокорейской ракеты KSLV-1. На разгонном блоке КВТК мы хотим установить новую БЦВМ «Бисер-7». От предыдущей модели ее будет отличать: повышенная в два раза вычислительная производительность; возможность работать с числами, представленными в форме с плавающей запятой; универсальный высокоскоростной последовательный интерфейс; увеличенный объем памяти; уменьшенные массово-габаритные характеристики. Для «Бисера-7» уже разработан центральный процессор и создаются еще более интегрированные БИС. Если смотреть совсем далеко, то ориентир для НПЦ АП – разработка БЦВМ с использованием технологии «система на кристалле». ДИректор предприятия, доктор технических наук Ефим Леонидович Межирицкий. ссылка **Аскет 2**4 декабря 2013 00:39 **1** Цитата: Орда штук 20? значит 20 микросхем бисер3 уже сделали, неплохо, но где компутеры на бисерах? и знаете почему ,потому ,что на МБР лишних 20-30кг не вопрос,а вот для дома... На западе микросхемы делятся на категории commercial, industrial, military и

space.

В России — все разделено несколько по другому: микросхемы продаются с приемкой 1 (т.н. приемка ОТК — отдела технического контроля, когда сам завод тестирует микросхемы), приемкой 5 (приемка заказчика, в случае военных военный представитель контролирует тесты) и приемка 9 (когда к работам привлекается только наиболее квалифицированный персонал — для космоса и ядерных электростанций). Сама по себе приемка 5/9 не означает, что микросхема радиационно-стойкая — стойкость к спец.факторам указывается в (не публичной) документации на микросхему.

Вот эти дополнительные тесты, керамический корпус и мелкосерийное производство (когда стоимость разработки делится не на 1млн микросхем, а на 100) и приводят к тому, что военная/космическая микросхема стоит минимум в 10 раз дороже гражданской, а максимум — может и по 100'000\$ за штуку стоить.

Однако не любую микросхему можно поставить в Российскую военную технику существует список отечественных (в «отечественные» входят и Белорусские микросхемы из Интеграла) электронных компонент, которые можно использовать при создании техники, где все перечислено поименно. Если какой-то завод создает новую микросхему — то до попадания в этот список её нельзя будет использовать.

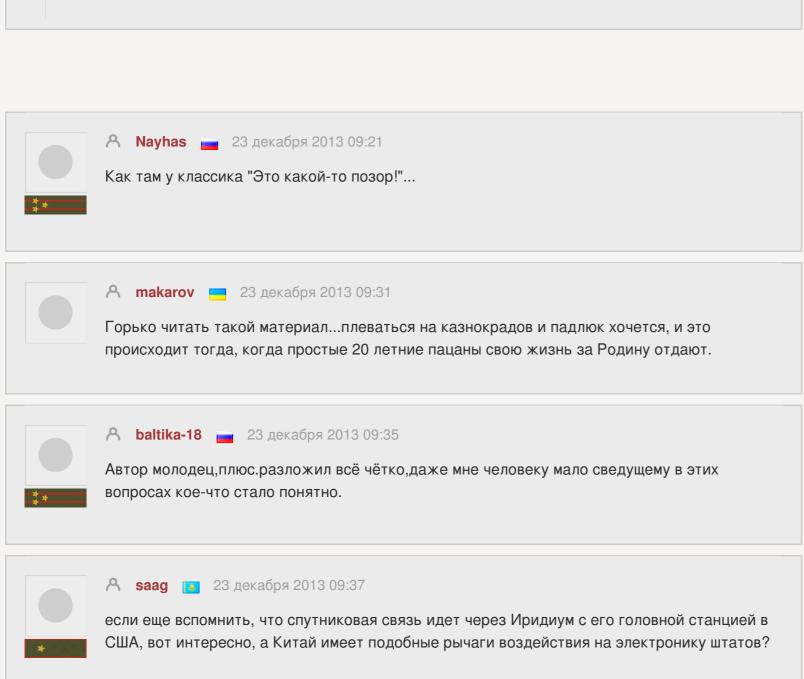
Использование импортных микросхем требует индивидуального разрешения (с соответствующей формальной бюрократией о том, что отечественных аналогов

МОП на текущий год не нашел вот на 2011 можно скачать тут

нет, но как появятся — обязательно будем их использовать).

Перечень МОП 44.001 является официальным изданием Министерства обороны Российской Федерации и обязательным для всех организаций, предприятий и учреждений, независимо от форм собственности, осуществляющих разработку (модернизацию), производство, эксплуатацию и ремонт аппаратуры военного назначения по заказу Министерства обороны Российской Федерации, для органов военного управления, научно-исследовательских организаций и военных представительств Министерства обороны Российской Федерации, а также для разработчиков и изготовителей изделий.

Noffchik7691 23 декабря 2013 22:58 1 Это уже похоже не на отсутствие порядка, а на ЗАКОНОМЕРНОСТЬ! В "аргументах недели" была статья что единственный в стране институт который исследовал технику, программы и радиоэлементы на предмет "закладок" два года назад благополучно закрыт! Слава нашим дальновидным руководителям! Аскет 24 декабря 2013 00:42 1 Цитата: voffchik7691 В "аргументах недели" была статья Не читайте на ночь рукопожатный бред подобных изданий... ОАО «Росэлектроника» выполняет проект по созданию высокотехнологичного научно-производственного комплекса межотраслевого центра проектирования, каталогизации и изготовления фотошаблонов. Проект реализуется в рамках Федеральной целевой программы «Развитие электронной компонентной базы и радиоэлектроники» на 2008-2015 годы. Противник больше не сможет поставить "закладки" в микросхемы, используемые в российском вооружении A studentmati ___ 24 декабря 2013 00:51 ↑ Цитата: Аскет Цитата: voffchik7691 В "аргументах недели" была статья Не читайте на ночь рукопожатный бред подобных изданий... Свежо предание, но верится с трудом. Из того что знаю и понимаю, вижу, что не хватает мощностей для "прочёса". 🖰 studentmati 📥 24 декабря 2013 00:51 🕇 Цитата: Аскет Цитата: voffchik7691 В "аргументах недели" была статья Не читайте на ночь рукопожатный бред подобных изданий... Свежо предание, но верится с трудом. Из того что знаю и понимаю, вижу, что не хватает мощностей для "прочёса". AVV = 5 января 2014 12:42 ↑ Когда будут наказывать за головотяпство чиновников,государственных структур,в том числе силовых!!!Кто торгует гос.тайной или дает разрешение на использование такой аппаратуры в войсках и других гос.структурах!!!Одни зарабатывают деньги,а другие не принимают никаких мер,для противодействию легальному шпионажу!!!Нужно не только увольнять без пенсий ,таких начальников,но и привлекать к уголовной ответственности!!!



🔼 RDS-1 🧫 23 декабря 2013 14:45 🕇 Цитата: saag интересно, а Китай имеет подобные рычаги воздействия на электронику штатов? Да вот же, на любимом сайте в прошлогодней статье "В США в чипе китайского

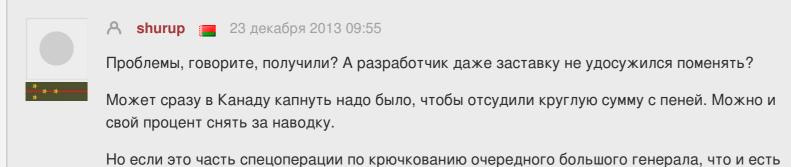
производства обнаружен бэкдор" читаем:

Китайский бэкдор ("чёрный ход", незадокументированные возможности) был обнаружен в процессоре, на территории США, по ходу исследования, которое было проведено в связи с заявлениями некоторых разведывательных агентств, таких как MI5 и АНБ, что микросхемы могут содержать "закладки", помещённые туда производителями.

Чип - Microsemi/Actel ProASIC3 широко используется во многих системах, включая атомные станции и общественный транспорт. Отличие версии ProASIC3 в "военном" исполнении состоит в лучшей устойчивости к радиационному и электромагнитному воздействию, а так же перепаду температур, конструкция полностью совпадает с "гражданской" версией.

После проверки чипа на наличие "нетипичных функций" был обнаружен бэкдор, помещённый туда фирмой изготовителем, и способный снять крипто защиту с микросхемы, поменять ключ кодировки AES, получив доступ к незашифрованному потоку данных или вызвать **значительные неполадки в работе**, то есть использоваться как своеобразный "мастер ключ", работе которого не мешал даже факт защиты конфигурации ключом официального пользователя

Честно говоря, я бы сильно удивился, если бы закладок не оказалось ;) Китайцам надо быть полными лохами, чтобы, имея возможность, их не сделать.



"безопасность государства по-русски", то будут ещё проблемы.

Мне понравилась буханка связи с летунами. Надеюсь, что в ней много разноцветных лампочек для начальства.





A hohryakov066 a 23 декабря 2013 10:12 Это не просто позор - это полный ! То, что наше доблестное АБВГД балуется коммерцией я знаю, до такой степени!

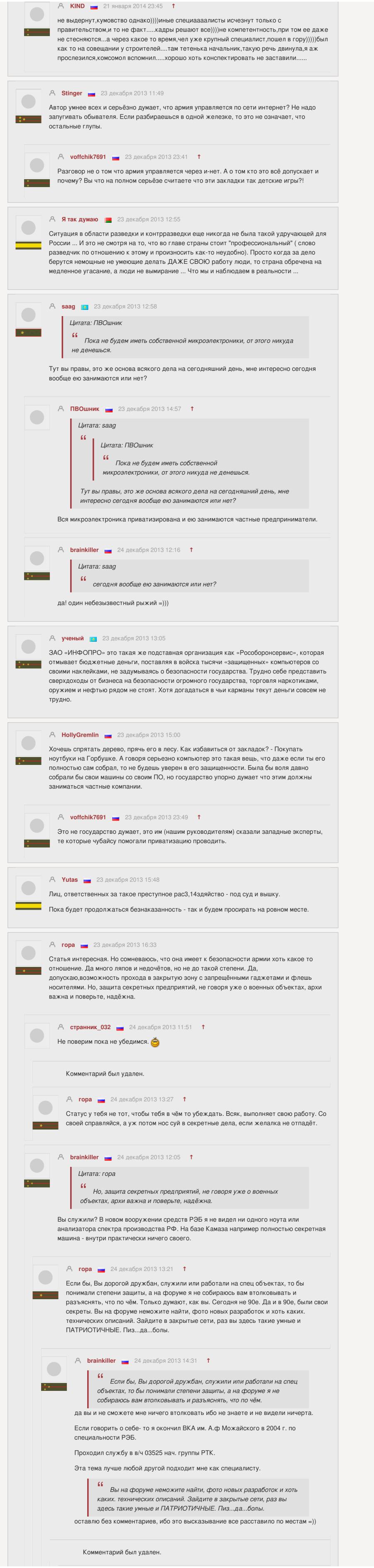




подпускать к этой теме. К сожалению практика последних лет привела к процессу

по зернышку выдергивать всю эту шушеру из процесса.

вымывания настоящих профессионалов в угоду безмозглому планктону... печаль однако. Хотя на мой взгляд не все потеряно, главное чтобы соответствующие службы начали хоть



не обошлось, и тут.

Жди в гости. Гражданин.

балаболов как вы в гости не жду.

Я не боюсь говорить правду с открытым забралом это видимо вас и бесит.

Комментарий был удален.



A aud13 📥 23 декабря 2013 16:44

фирмой созданной с зарубежным участием?

Раздолбайское отношение к информации, к сожалению, осуществляется у нас во многих местах.

Так к примеру знаете ли вы что у нас аудитором Банка России является ЗАО "Прайс Уотерхаус Куперс" - дочернее предприятие одного крупнейших зарубежных аудиторов.

Как Вы считаете, возможно ли чтобы аудитором Федеральной резервной системы США стала дочерняя фирма какой-нибудь российской аудиторской компании?

Я так понимаю что и на пушечный выстрел не подпустили бы нас к ихним документам.

Еще вопрос - а зачем Банку России нужно аудиторское заключение выданное именно

Ну понятно экспорто ориентированное предприятие для заключения контрактов, с подготавливает аудиторское заключение для того чтобы показать контрагентам.

Если так дело и дальше пойдет то скоро и кабинет министоров России, министерство обороны и администрацию президента будут очень внимательно проверять иностранные

Наших аудиторов кстати, на протяжении последних нескольких лет успешно гнобит выходец из этой самой Прайс Уотерхаус Куперс"



аудиторы.

🖰 yanus 🔛 23 декабря 2013 17:01

Забавная статья. Автор развел "скандалы, интриги, расследования", но вот проверить не смог))

К сожалению, машина не была подключена ни к Интернету ни к локальной сети, поэтому не удалось посмотреть сетевую активность на IP адресах, чтобы выяснить в каком состоянии находится сервис фирмы Absolute Software.

Ну, да. Только на скрине почему-то горят значки сетевых подключений.))) По wifi, который вроде как есть в этой железке, тоже не к чему было подключится?)))

Такого унылого "черного" пиара конкурентов давно не видел.



Автор хотел отследит активность в интернете, а МВК подключен к локалке.ИМХО



А странник_032 23 декабря 2013 18:40

Если дело обстоит действительно так, как рассказывает автор статьи я не сколько не удивляюсь.

Как гласит поговорка "У каждой недоработки есть имя и фамилия",дедушку Сталина сейчас модно хаять и обливать помоями,но при нём за такой бардак давно бы "пломбу" в затылок всем виновным поставили.

Не верю что в нашей стране нельзя найти хороших спецов по IT,которые могут создать ОС и др.необходимые программы,так необходимые для ВС России.

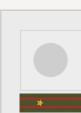
Что же касается "железа",то я думаю и многие люди со мной согласятся,всё это можно производить и в России(была бы воля и желание).

P.S.Одно радует что "комп" в пыли был,видать им и не пользовались толком(может те кто должен с ним работать имеет в голове мозги и не стал им пользоваться,понимая чем пользование сим девайсом пахнет).



A uzer 13 📥 23 декабря 2013 19:11

Проблема закладок и шпионажа существует и с каждым годом будет усугубляться.В России отсутствует производство собственных компьютеров и элементной базы. Это еще значит, что в полном объеме нельзя проверить иностранные изделия на наличие шпионских модулей и программ. Нет такого оборудования и такой службы. Специалистов также не хватает, да и не уважают их в нашем обществе, таков уж менталитет. Если человек не копает землю лопатой и не таскает бревна на спине, то значит он не шибко занят и является первым кандидатом на сокращение. Если уж ноутбуки для нужд армии закупаются за рубежом, то их надо сразу отправлять на переделку. В первую очередь надо написать свой БИОС и удалить тот, который был в компьютере. Ничего сложного в этом нет, БИОС-это базовая система ввода-вывода. Это программа, которая определяет очередность загрузки модулей, контроллеров и служб. Модули ТРМ следует сразу удалить, то же самое сделать с сетевым контроллером. Если кому нужен будет выход в интернет (а не всем желающим)-путь подают заявку на активацию сетевого контроллера. Локальные сети-это тоже хорошо. Но если рядом с локальным компьютером валяется ноутбук неизвестного происхождения с активированным интернет-соединением(а то и с подключенным USB модемом)-это уже плохо.



А невидимка 23 декабря 2013 20:25

И это в стране,которая обладала всем необходимым комплексом в сфере высоких технологий!

Очень ценен и правилен вывод: все об этом знают. Это предательство, государственная измена, назовите как хотите. По законодательству это срок и не малый. Сколько на руках у населения электроники?

Неужели производство элементарной базы. не выгодно? Впрочем и отдавать стратегические отрасли в руки частника это не дело..



A DocKlishin 23 декабря 2013 20:47

Спасибо автору за статью. Очень понравилась. Написал бы сам, что то похожее но не являюсь специалистом в данной области. Только любитель гаджетов. Про закладки эт все понятно и давно об этом знают. Потому описанный факт, как разгильдяйство и измена Родине никак по другому назвать нельзя. Чего далеко ходить, те же америкосы обоср...лись, когда закупили компы на элементной базе китайцев. ПОЖЕЛАНИЕ к автору если будет время, напишете пожалуйста обзор по НАШЕЙ Российской электронной промышленности. Насколько мне известно у нас есть предприятия такие как АНГСТРЕМ, МЦСТ. И те и другие входят в корпорацию Российская электроника (кажется так называется). Отстаем нормально, но для нужд армии выпускать всю линейку можем. В 2010 г закупили у немцев (АМD) подержанный завод, будем переходить на 90 нм. Сейчас 130 нм. Мир переходит на 32, а некоторые товарищи и на 20 нм.



A DocKlishin 23 декабря 2013 20:54

С этого года начали выпускать процессоры Мультиклет. Жаль только, что делают их в Азии. С моей точки зрения развитие электронной промышленности - вопрос больше политический. Нах...й олимпиаду, универсиаду, ЧМ по футболу (эт так вообще смех). А деньги пустить на развитие высоких технологий. Хотя бы для начала создать свой качественный комп устроенный полностью на отечественной элементной базе. Софт разработать сможем САМИ - вот в этом я нисколько не сомневаюсь. И продавать в добровольно принудительном порядке в школы, поликлиники, больницы. Нашим братьям в СНГ. Только в этом случае что то может получиться. Что, касается меня лично, то я бы с удовольствием взял отечественный продукт. А так Китай китай китай... Движемся в нужном направлении, но медленно. Да и потом.... что тиснуть технологию нельзя в конце то концов....



А невидимка 23 декабря 2013 21:58 ↑

Мне кажется не движемся. Бизнес делает какие-то потуги...для извлечения прибыли.

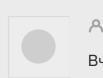
Отверточная сборка, без базы пустая трата сил (для госинтересов). а вот, что вопрос политический, это вы в точку.

Только у нас, что не вопрос, то политический.

Да и политика какая-то тухлая..

Небольшое видео с выставки Новая электроника 2013.





A voffchik7691 a 23 декабря 2013 22:37

Вчера, в рамках статьи "Угроза пятого элемента", люди долго спорили (вплоть до оскорблений) что плохо что в наших новейших разработках присутствуют зарубежные радиоэлементы.

то может отключить "изделие", так перед этим этот кто-то узнает всё что надо!
Вот всё становится на свои места - Булава чаще падает чем летает, и спутники не желают

Данная статья прямое подтверждение этого, только по моему ещё хуже. Мало того что кто-

следовать на орбиту! Кстати, а почему если наша ракета-носитель стартует со спутниками америкосов, всё

Кстати, а почему если наша ракета-носитель стартует со спутниками америкосов, всё нормально! А вот если только наши, то ...

Комментарий был удален.

Комментарий был удален.



A brainkiller 24 декабря 2013 12:22

Цитата: КПА

СС Автор хотел отследит активность в интернете, а МВК подключен к локалке.ИМХО

Одно только наличие вайфая говорит об отсутствии должной проверки машины.

Или 010 в армии отменили полностью.



КПА ___ 26 декабря 2013 00:26 ↑

Ну,АСУ ТЗ на вайфае и построено,о роли спецприказов можно судить по разрешенным мобильникам для срочников.



А гора 24 декабря 2013 13:34

С одной стороны кажется что где, где но на этом то форуме не дураки собрались, а нет и без них не обошлось, и тут. Да сама суть новых разработок, без сикретки, сама по себе и существовать не может. И первое, это безопасность, а уж потом и всё остальное.



А Takashi ___ 24 декабря 2013 18:31

"Для незнающих поясню, спецпроверка и специсследования это необходимые процедуры (и очень дорогостоящие) для того, чтобы техника появилась на секретных объектах и в войсках. После этих проверок техника считается безопасной с точки зрения утечек секретной и конфиденциальной информации и может использоваться на секретных и защищенных объектах."

я однажды видел как печатные машинки (60-гг выпуска) проверяли. Долго ржал про себя.

И как тебя еще не взяли за цугундер, ведь ты сфотал супер секретную машинку :):):):

У меня вопрос возник, а если я за рубежом приобрету для личного пользования компьютер с чипом TRM - компьютер заберут на таможне или ко мне придут люди в черном и впаяют срок?



A studentmati ___ 25 декабря 2013 00:13 1

Цитата: Takashi

У меня вопрос возник, а если я за рубежом приобрету для личного пользования компьютер с чипом TRM - компьютер заберут на таможне или ко мне придут люди в черном и впаяют срок?

Никогда нельзя недооценивать противоположную сторону! Всё ввозится и широкомасштабно продаётся и используется! В том числе технологии TRM! На благо России.

Комментарий был удален.

© 2010-2017 «Военное обозрение»

Свидетельство о регистрации СМИ Эл № ФС77-56354, выдано 02.12.2013 г. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Правила использования и копирования информации с сайта

«Правый сектор» (запрещена в России), «Украинская повстанческая армия» (УПА) (запрещена в России), ИГИЛ (запрещена в России), «Джабхат Фатх аш-Шам» бывшая «Джабхат ан-Нусра» (запрещена в России).

Пользователю

Главная Реклама і

Реклама на сай Контакты

Прави

Форум

Мы в соц.сетях

Ţ Twitte

© Одноклассники в ВКонтакте

Google+

Youtul