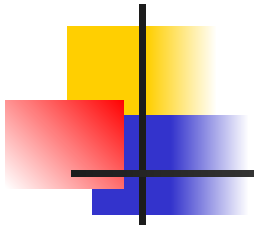
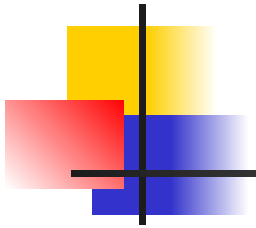
Избавление от троянов-вымогателей и разблокировка Windows

Борисов В.А.
КАСК – филиал ФГБОУ ВПО РАНХ и ГС
Красноармейск 2013 г.

Оглавление

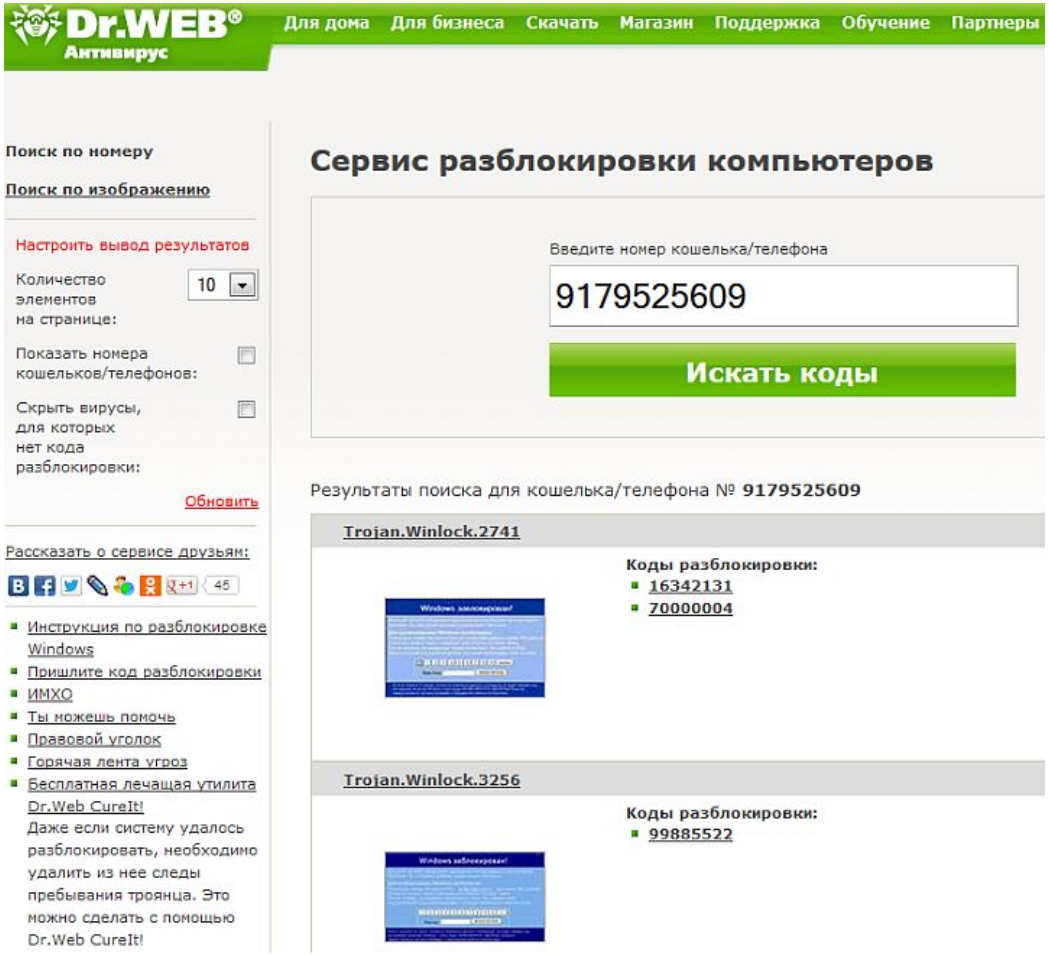


Голыми руками

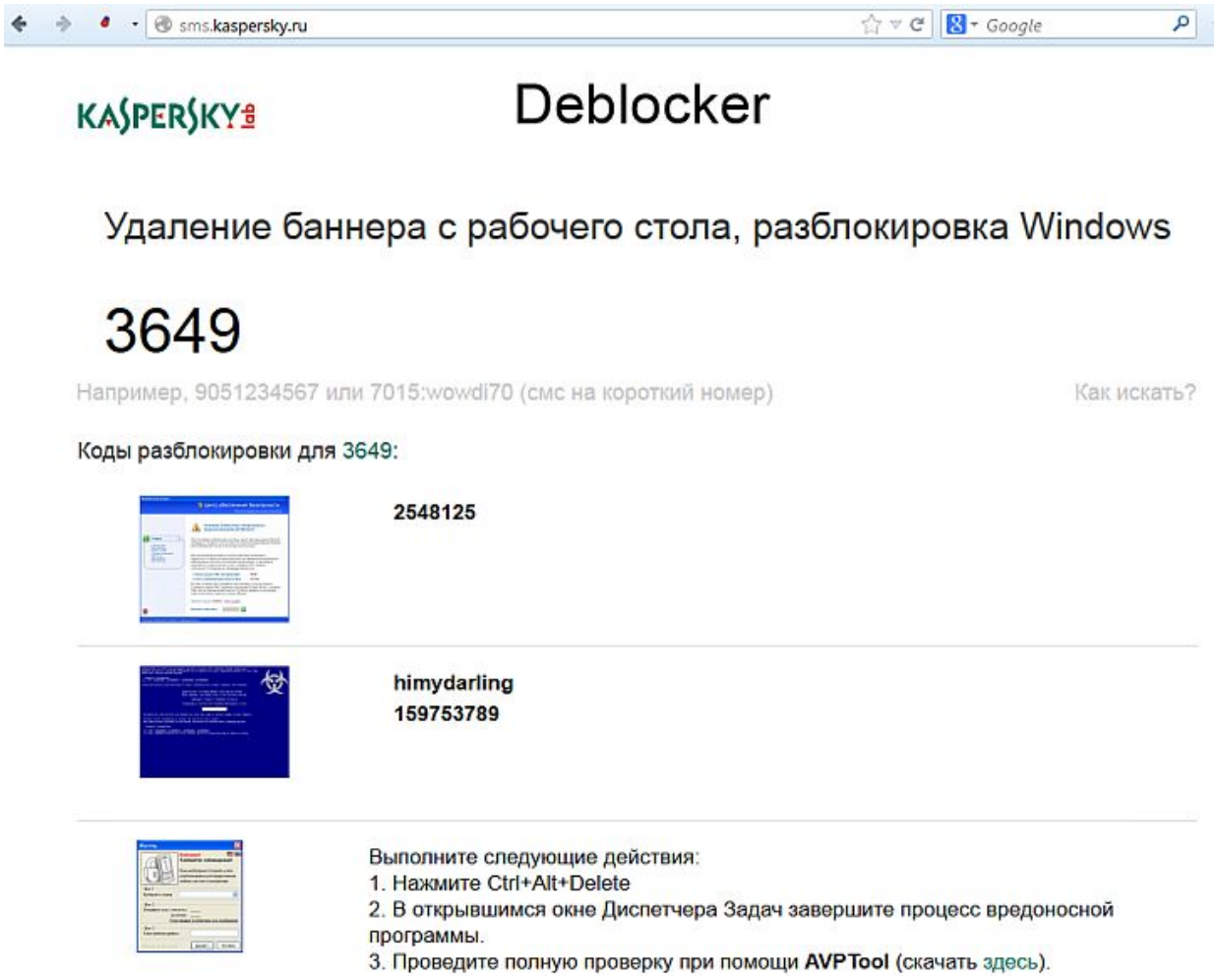


- Для некоторых троянов действительно существует код разблокировки.
- В редких случаях они даже честно удаляют себя полностью после ввода верного кода.
- Узнать его можно на соответствующих разделах сайтов антивирусных компаний.

Сервис разблокировки Windows компании «Доктор Веб»

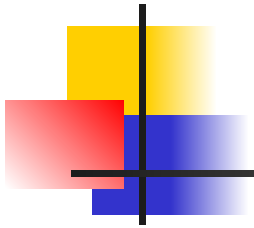


Сервис разблокировки Windows компании «Лаборатория Касперского»

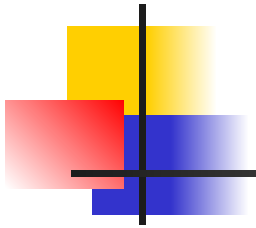


- Зайти в специализированные разделы сайтов «Доктор Веб»Зайти в специализированные разделы сайтов «Доктор Веб», «Лаборатории Касперского» и других разработчиков антивирусного ПО можно с другого компьютера или телефона.

- После разблокировки не радуйтесь преждевременно и не выключайте компьютер.
- Скачайте любой бесплатный антивирус и выполните полную проверку системы. Для этого воспользуйтесь, например, утилитой Dr.Web CureIt!Скачайте любой бесплатный антивирус и выполните полную проверку системы. Для этого воспользуйтесь, например, утилитой Dr.Web CureIt! или

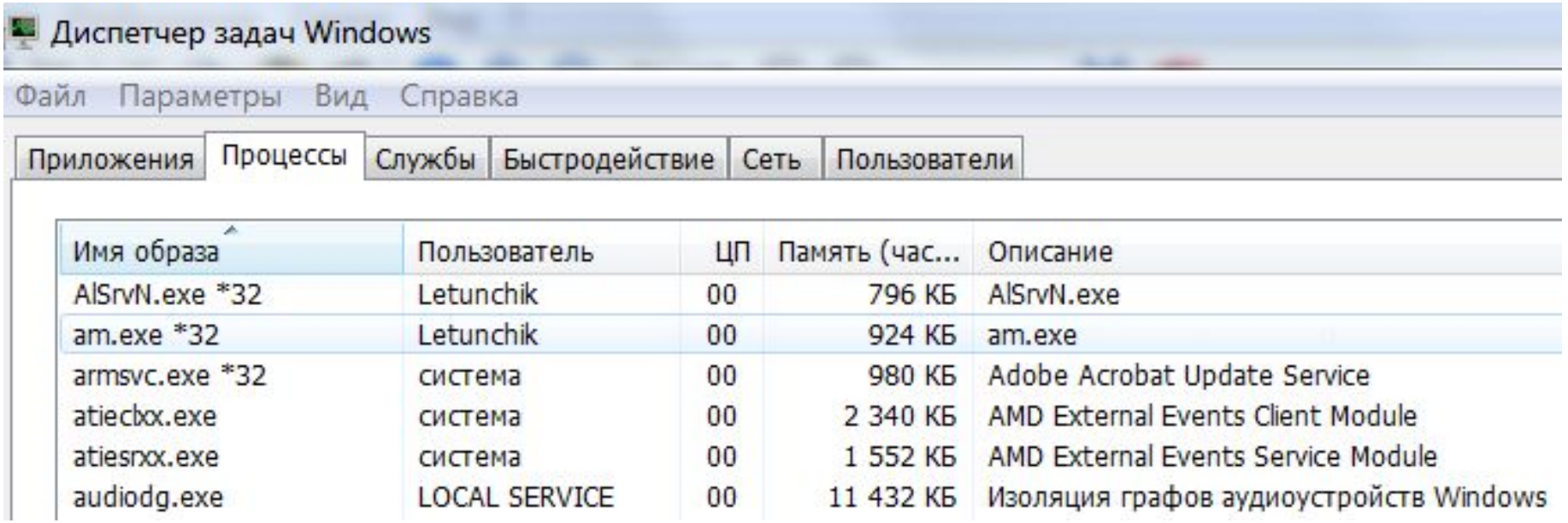


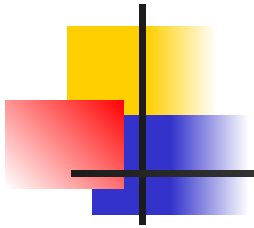
Простые меры



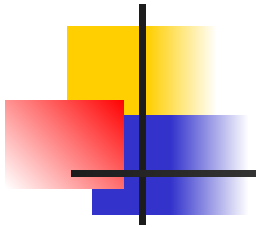
- Прежде чем использовать сложные методы и спецсофт, попробуйте обойтись имеющимися средствами.
- Вызовите диспетчер задач комбинацией клавиш {CTRL}+{ALT}+{DEL} или {CTRL}+{SHIFT}+{ESC}.
- Если получилось, то мы имеем дело с примитивным трояном, борьба с которым не доставит проблем. Найдите его в списке процессов и принудительно завершите.

Подозрительный процесс в диспетчере задач



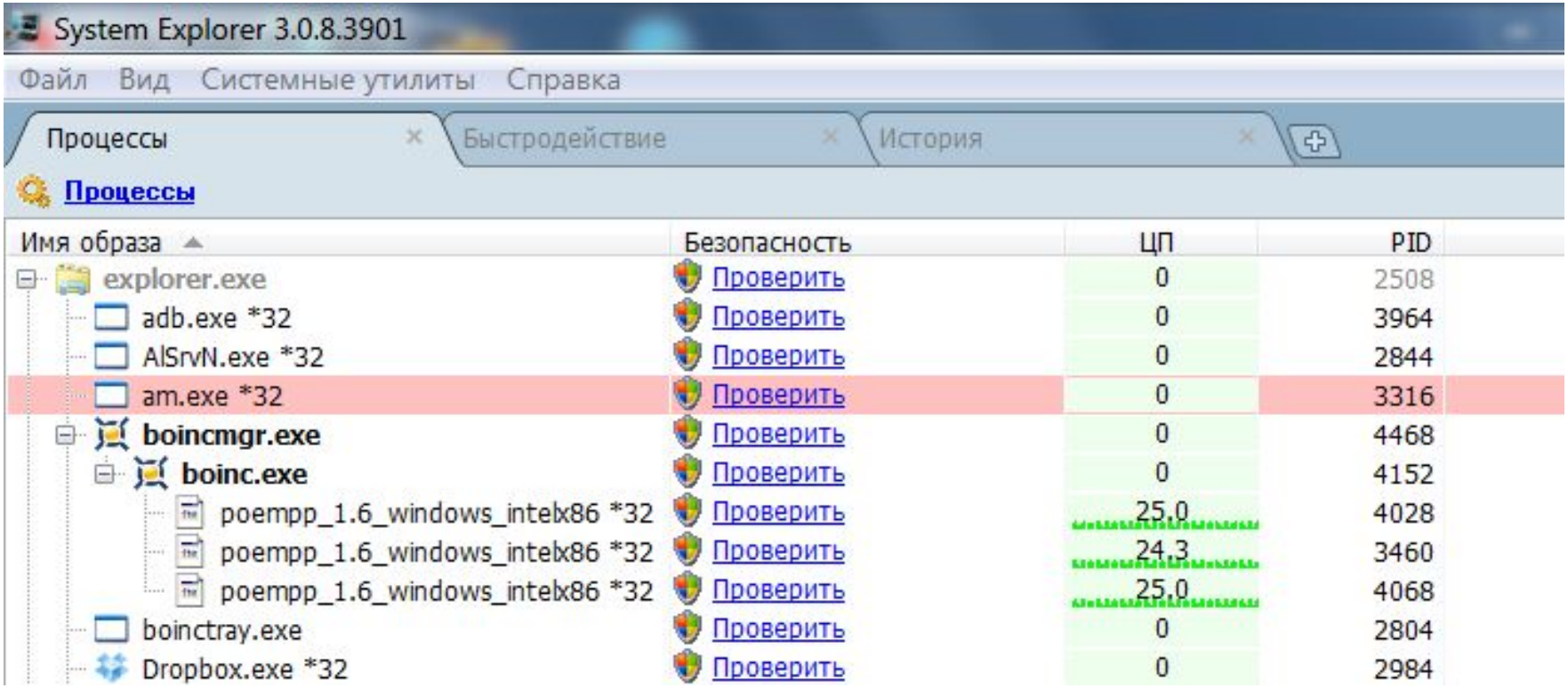


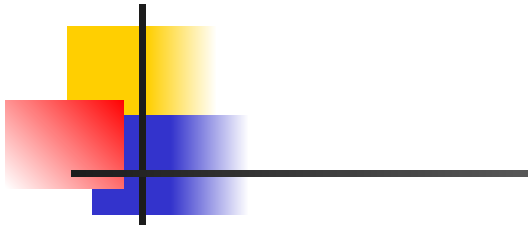
- Посторонний процесс выдаёт невнятное имя и отсутствие описания.
- Если сомневаетесь, просто поочерёдно выгружайте все подозрительные до исчезновения баннера.



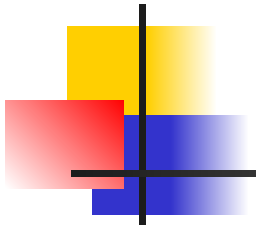
- Если диспетчер задач не вызывается, попробуйте использовать сторонний менеджер процессов через команду «Выполнить», запускаемую нажатием клавиш {Win}+{R}.

Подозрительный процесс в System Explorer

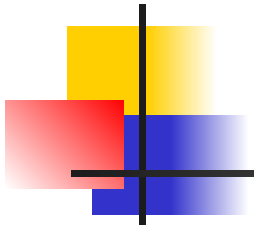




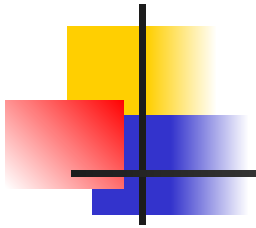
- Скачать программу можно с другого компьютера или даже с телефона. Она занимает всего пару мегабайт.
- По ссылке «проверить» происходит поиск информации о процессе в онлайновой базе данных, но обычно и так всё понятно.



- После закрытия баннера часто требуется перезапустить «Проводник» (процесс explorer.exe).
- В диспетчере задач нажмите: Файл -> Новая задача (выполнить) -> c:\Windows\explorer.exe.

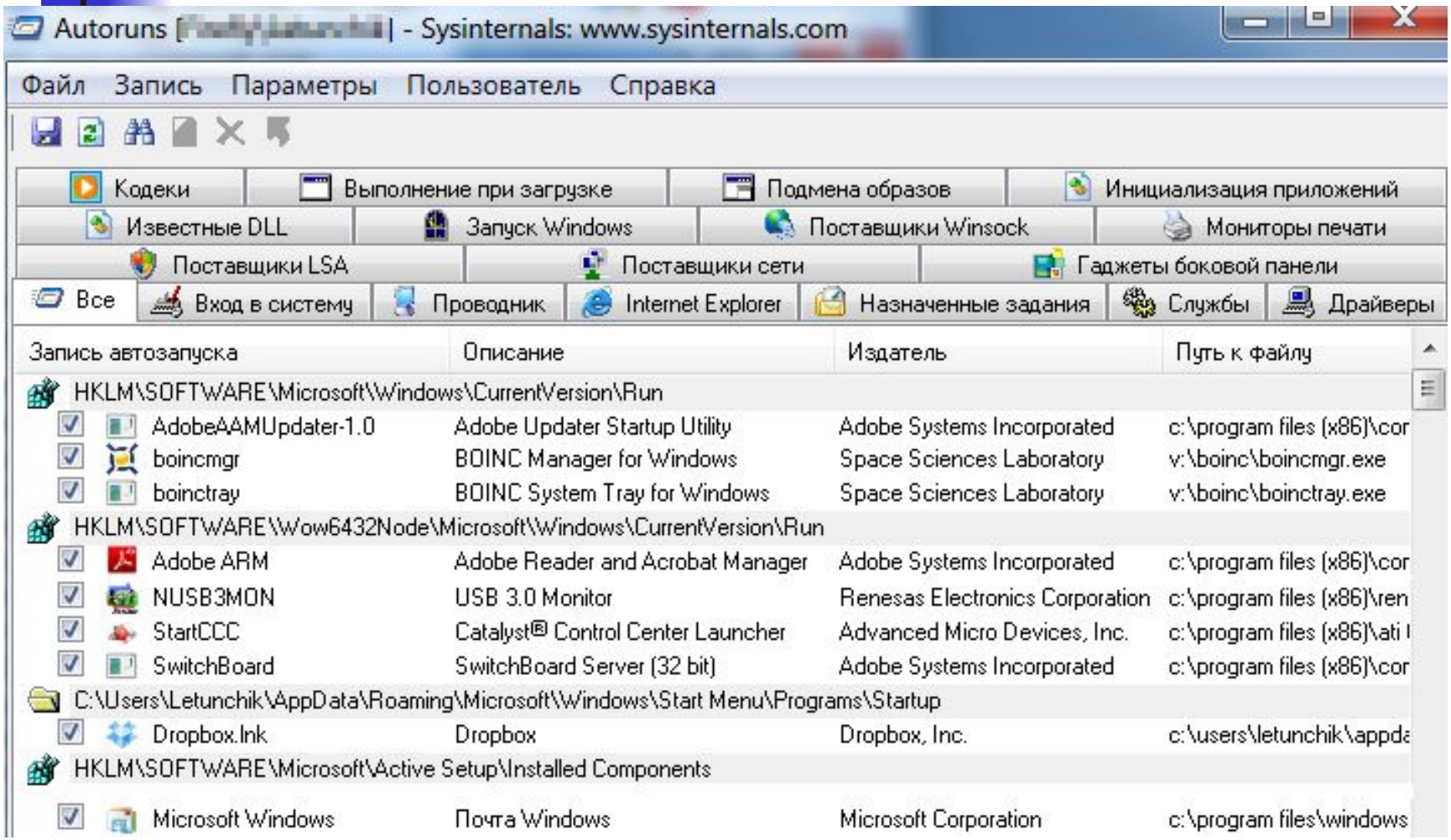


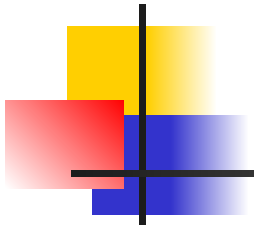
- Когда троян деактивирован на время сеанса, осталось найти его файлы и удалить их.
- Это можно сделать вручную или воспользоваться бесплатным антивирусом.



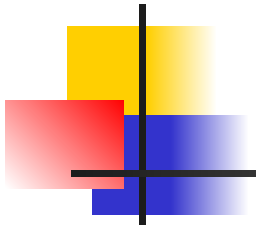
- Типичное место локализации трояна – каталоги временных файлов пользователя, системы и браузера.
- Целесообразно всё же выполнять полную проверку, так как копии могут находиться где угодно, а беда не приходит одна.

AutoRuns покажет все объекты автозапуска

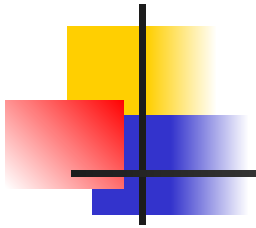




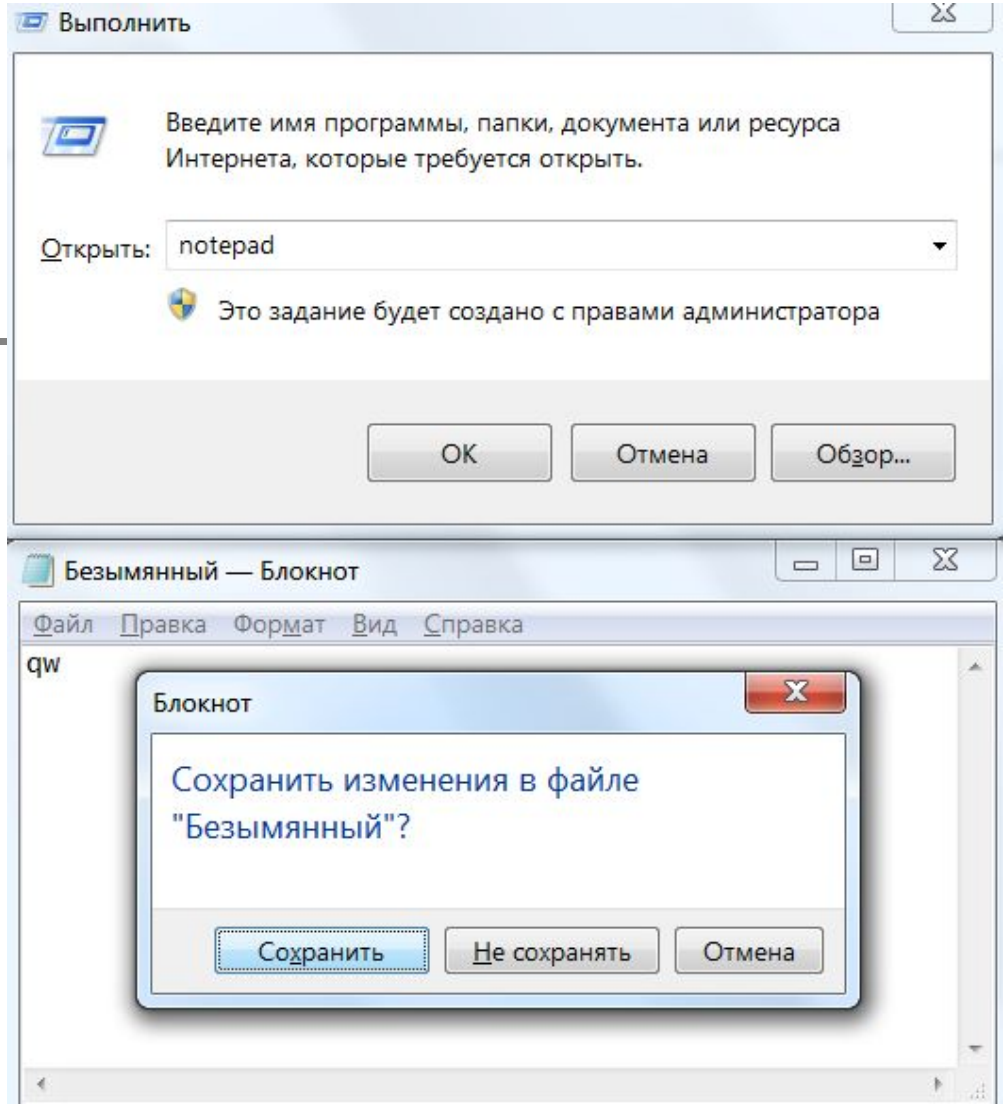
Хитростью



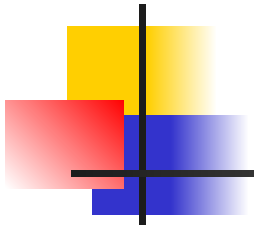
- Справиться с трояном на первом этапе поможет особенность в поведении некоторых стандартных программ.
- При виде баннера попробуйте запустить «вслепую» Блокнот или WordPad.



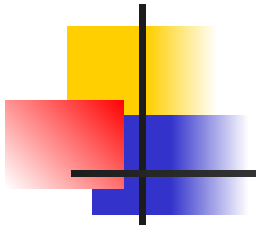
- Нажмите {WIN}+{R}, напишите notepad и нажмите {ENTER}.
- Под баннером откроется новый текстовый документ.
- Наберите любую абракадабру и затем коротко нажмите кнопку выключения питания на системном блоке.
- Все процессы, включая троянский, начнут завершаться, но выключения компьютера не произойдёт.



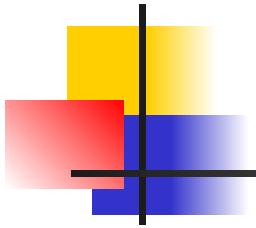
- Останется диалоговое окно «Сохранить изменения в файле?».
- С этого момента на время сеанса мы избавились от баннера и можем добить трояна до перезагрузки.



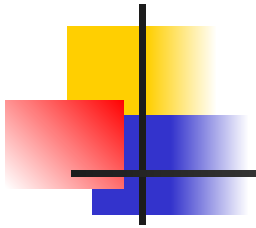
По старинке



- Более продвинутые версии троянов имеют средства противодействия попыткам избавиться от них.
- Они блокируют запуск диспетчера задач, подменяют другие системные компоненты.

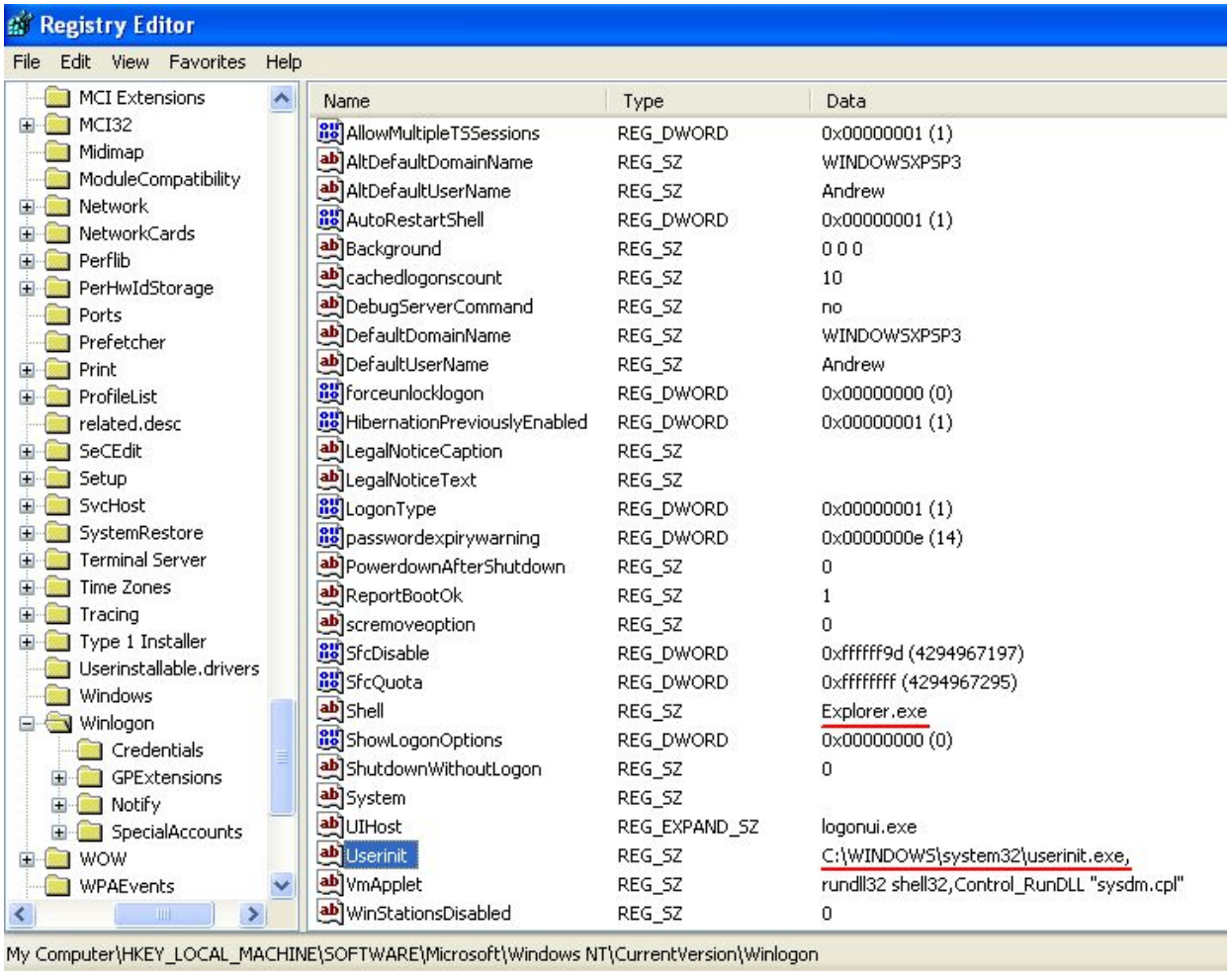


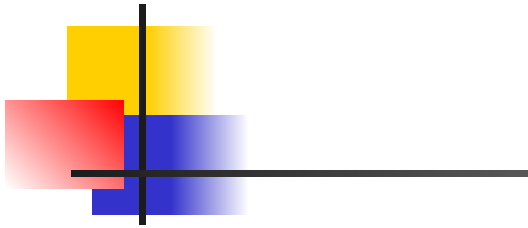
- В этом случае перезагрузите компьютер и удерживайте клавишу {F8} в момент загрузки Windows.
- Появится окно выбора способа загрузки.
- Нам требуется «Безопасный режим с поддержкой командной строки».



- После появления консоли пишем explorer и нажимаем {ENTER} – запустится проводник.
- Далее пишем regedit, нажимаем {ENTER} и видим редактор реестра.
- Здесь можно найти созданные трояном записи и обнаружить место, откуда происходит его автозапуск.

Ключи реестра, часто модифицируемые троянами семейства Winlock

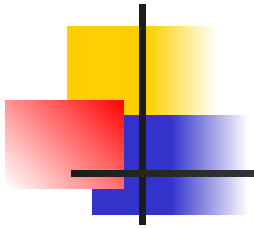




- Чаще всего вы увидите полные пути к файлам трояна в ключах Shell и Userinit в ветке

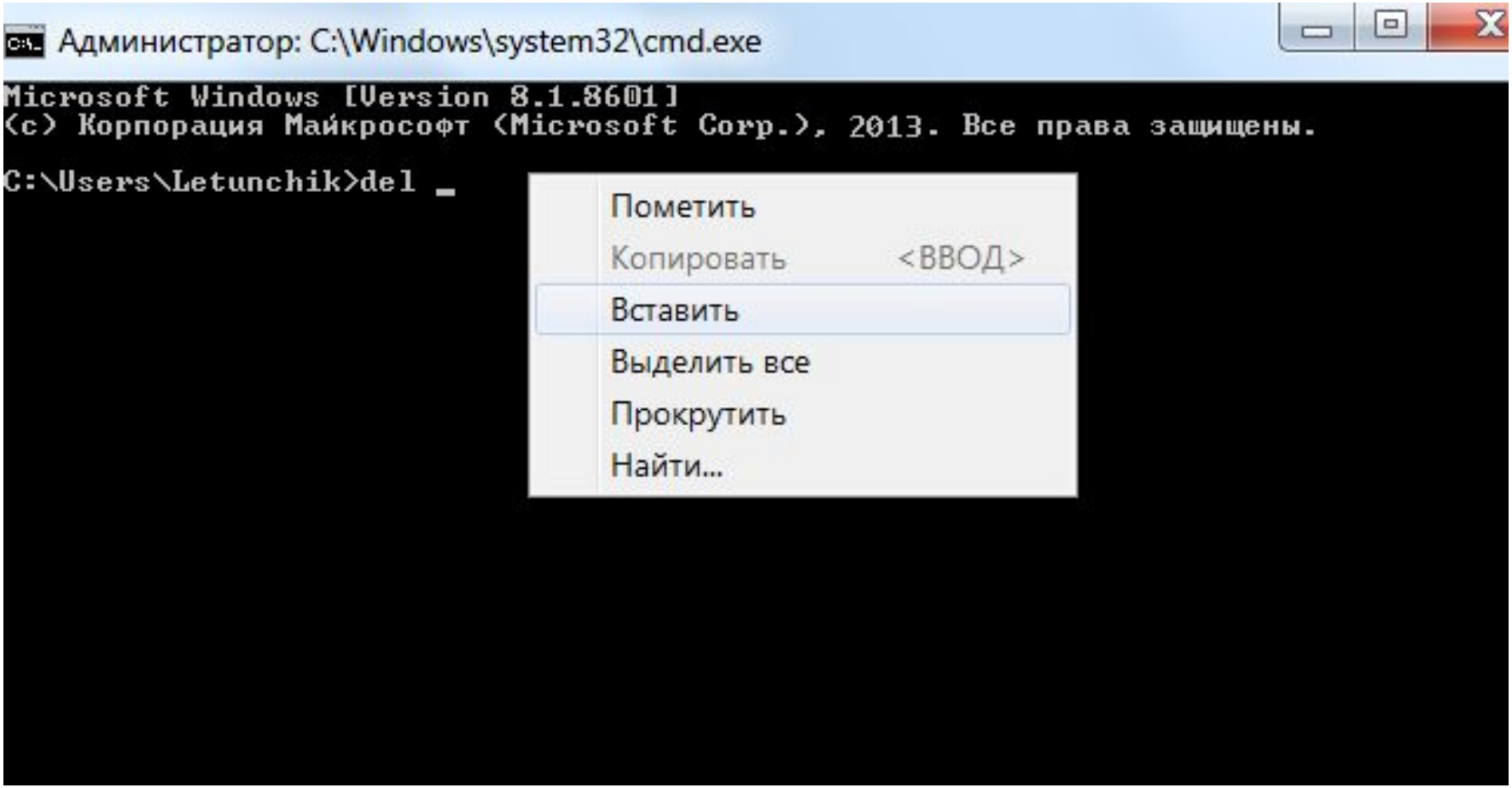
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

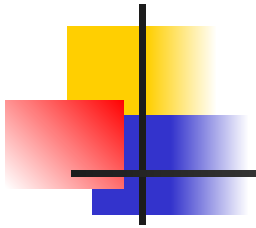
- В «Shell» троян записывается вместо explorer.exe, а в «Userinit» указывается после запятой.



- Копируем полное имя троянского файла в буфер обмена из первой обнаруженной записи.
- В командной строке пишем del, делаем пробел и вызываем правой клавишей мыши контекстное меню.

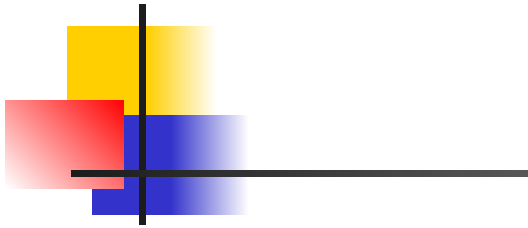
Удаление трояна из консоли





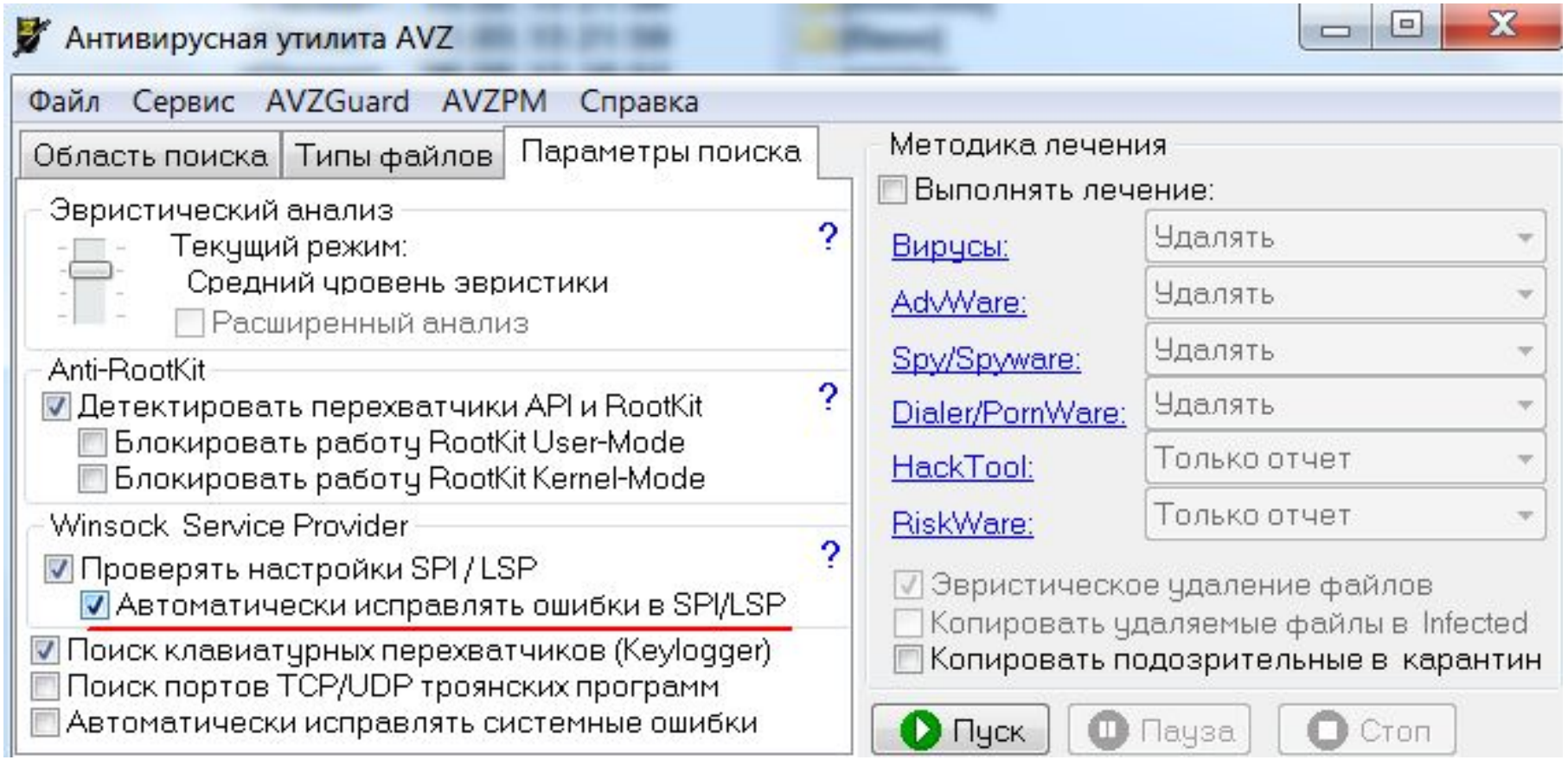
- Выбираем команду «вставить» и нажимаем {ENTER}.
- Один файл трояна удалён, делаем тоже самое для второго и последующих.

- Затем выполняем в реестре поиск по имени файла трояна, внимательно просматриваем все найденные записи и удаляем подозрительные.
- Очищаем все временные папки и корзину.
- Даже если всё прошло идеально, не поленитесь затем выполнить полную проверку любым антивирусом.

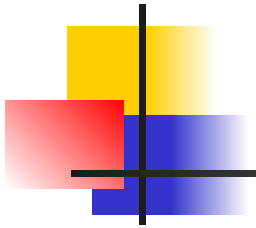


- Если из-за трояна перестали работать сетевые подключения, попробуйте восстановить настройки Windows Sockets API утилитой AVZ.

Восстановление сетевых сервисов с помощью AVZ



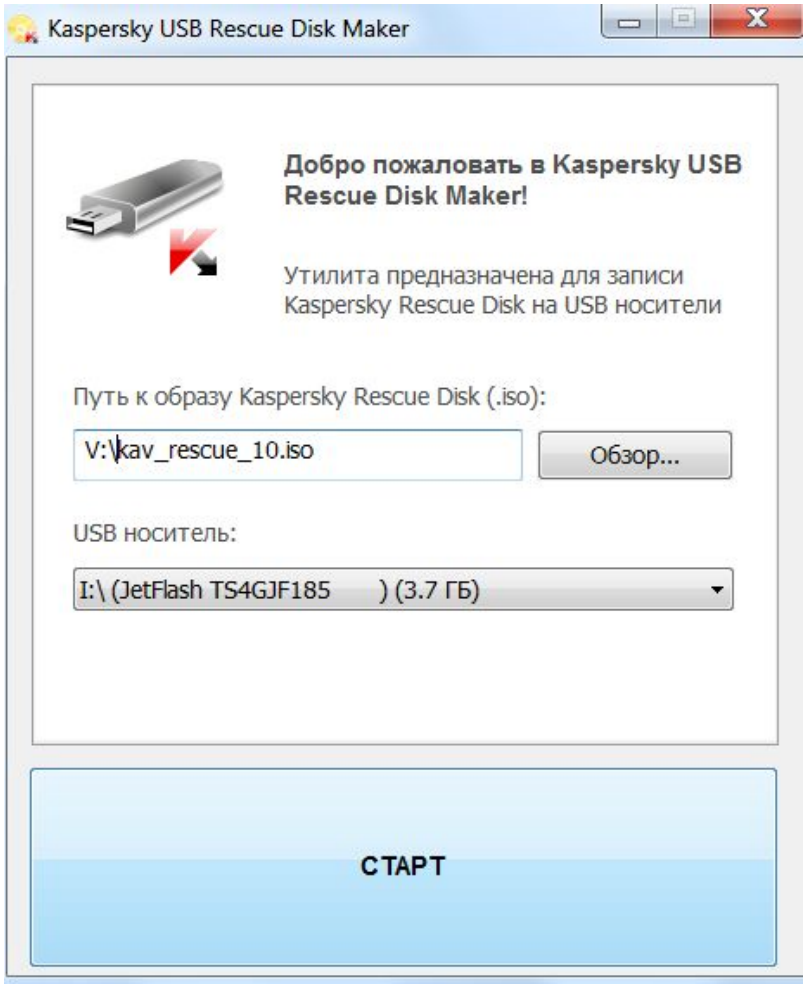
Операция

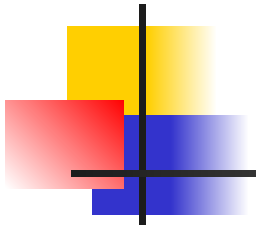


- В случаях серьёзного заражения бесполезно бороться из-под инфицированной системы.
- Логичнее загрузиться с заведомо чистой и спокойно вылечить основную.

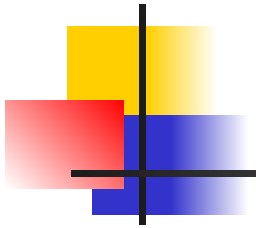
- Существуют десятки способов сделать это, но один из самых простых – воспользоваться бесплатной утилитой Kaspersky WindowsUnlocker, входящей в состав Kaspersky Rescue DiskСуществуют десятки способов сделать это, но один из самых простых – воспользоваться бесплатной утилитой Kaspersky WindowsUnlocker, входящей в состав Kaspersky Rescue Disk. Как и DrWeb LiveCD,

Создание загрузочной флэшки из образа Kaspersky Rescue Disk

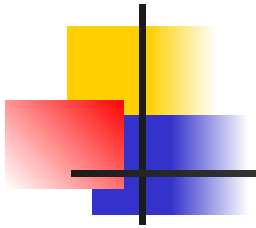




- При включении заражённого компьютера удерживайте клавишу для входа в BIOS.
- Обычно это {DEL} или {F2}, а соответствующее приглашение отображается внизу экрана.
- Вставьте Kaspersky Rescue Disk или загрузочную флэшку.



- В настройках загрузки выберите первым загрузочным устройством привод оптических дисков или флэшку (иногда она может отображаться в раскрываемом списке HDD).
- Сохраните изменения {F10} и выйдите из BIOS.

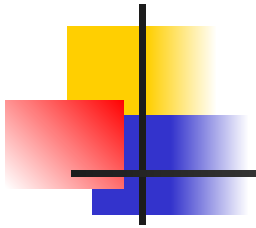


- Современные версии BIOS позволяют выбирать загрузочное устройство на лету, без входа в основные настройки.
- Для этого требуется нажать {F12}, {F11} либо сочетание клавиш – подробнее смотрите в сообщении на экране, в инструкции к материнской плате или ноутбуку.
- После перезагрузки начнётся запуск Kaspersky Rescue Disk.

Загрузка Kaspersky Rescue Disk

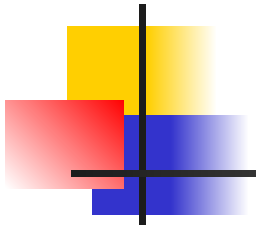
Kaspersky Rescue Disk в графическом режиме

Борьба на ранней стадии

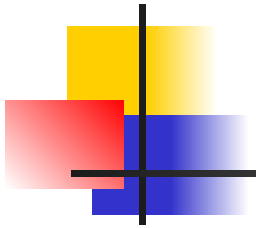


- Отдельный подкласс составляют трояны, поражающие главную загрузочную запись (MBR).
- Они появляются до загрузки Windows, и в секциях автозапуска вы их не найдёте.

Троян семейства Winlock, заразивший MBR



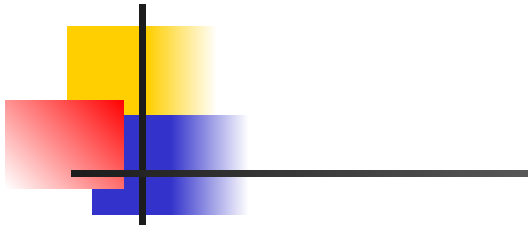
- Первый этап борьбы с ними заключается в восстановлении исходного кода MBR.
- В случае XP для этого загружаемся с установочного диска Windows, нажатием клавиши {R} вызываем консоль восстановления и пишем в ней команду fixmbr.
- Подтверждаем её клавишей {Y} и выполняем перезагрузку.



- Для Windows 7 аналогичная утилита называется BOOTREC.EXE, а команда fixmbr передаётся в виде параметра:

  Bootrec.exe/FixMbr

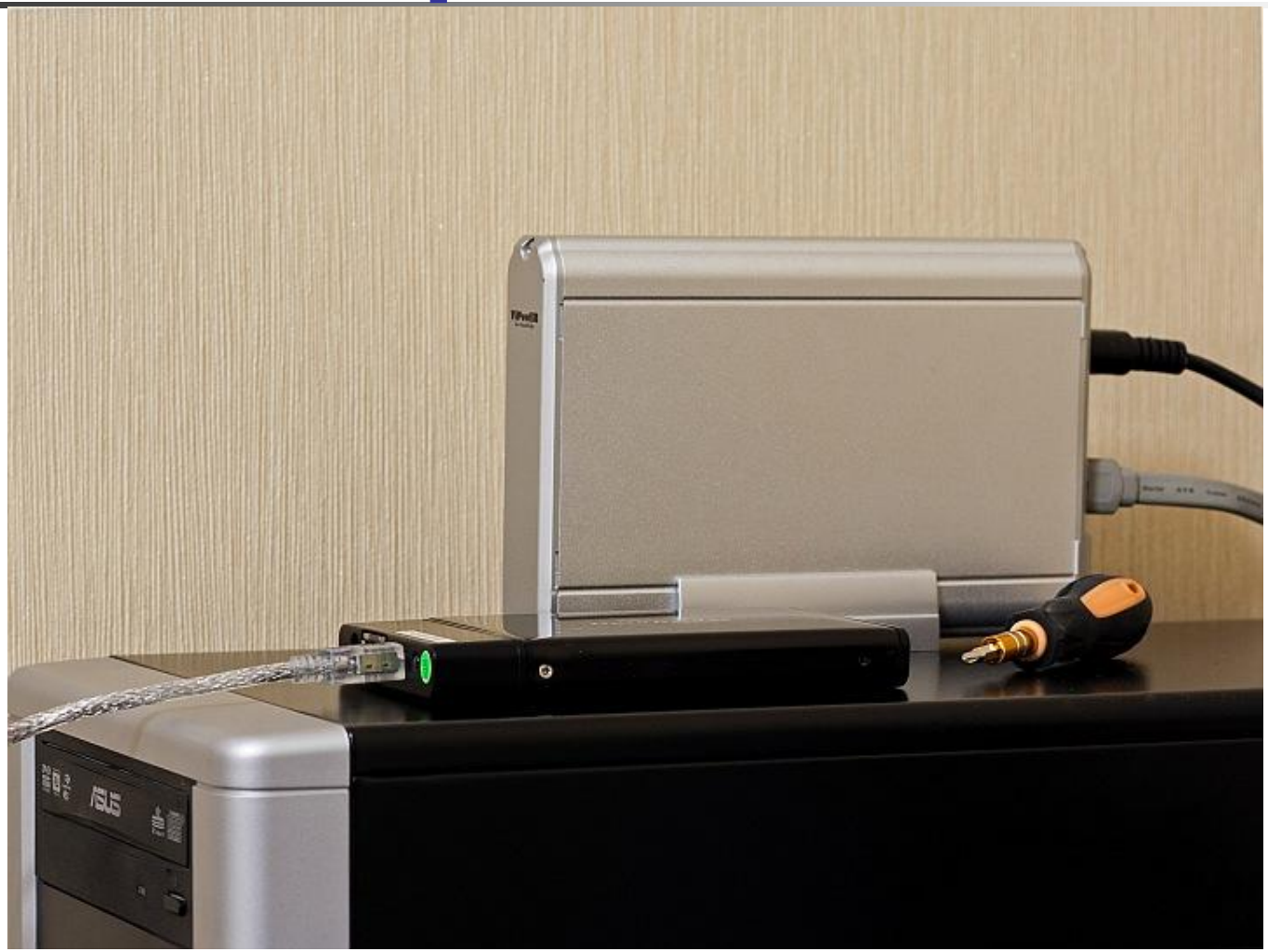
- После этих манипуляций система вновь загружается. Можно приступать к поиску копий трояна и средств его доставки любым антивирусом.

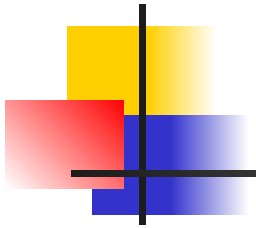


Отвертка

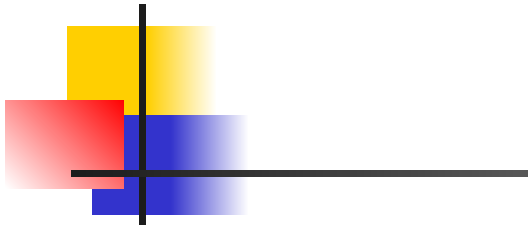
- На маломощных компьютерах и особенно ноутбуках борьба с троянами может затянуться, так как загрузка с внешних устройств затруднена, а проверка выполняется очень долго. В таких случаях просто извлеките заражённый винчестер и подключите его для лечения к другому компьютеру. Для этого удобнее воспользоваться боксами с

Антивирусная проверка жёстких дисков на другом компьютере



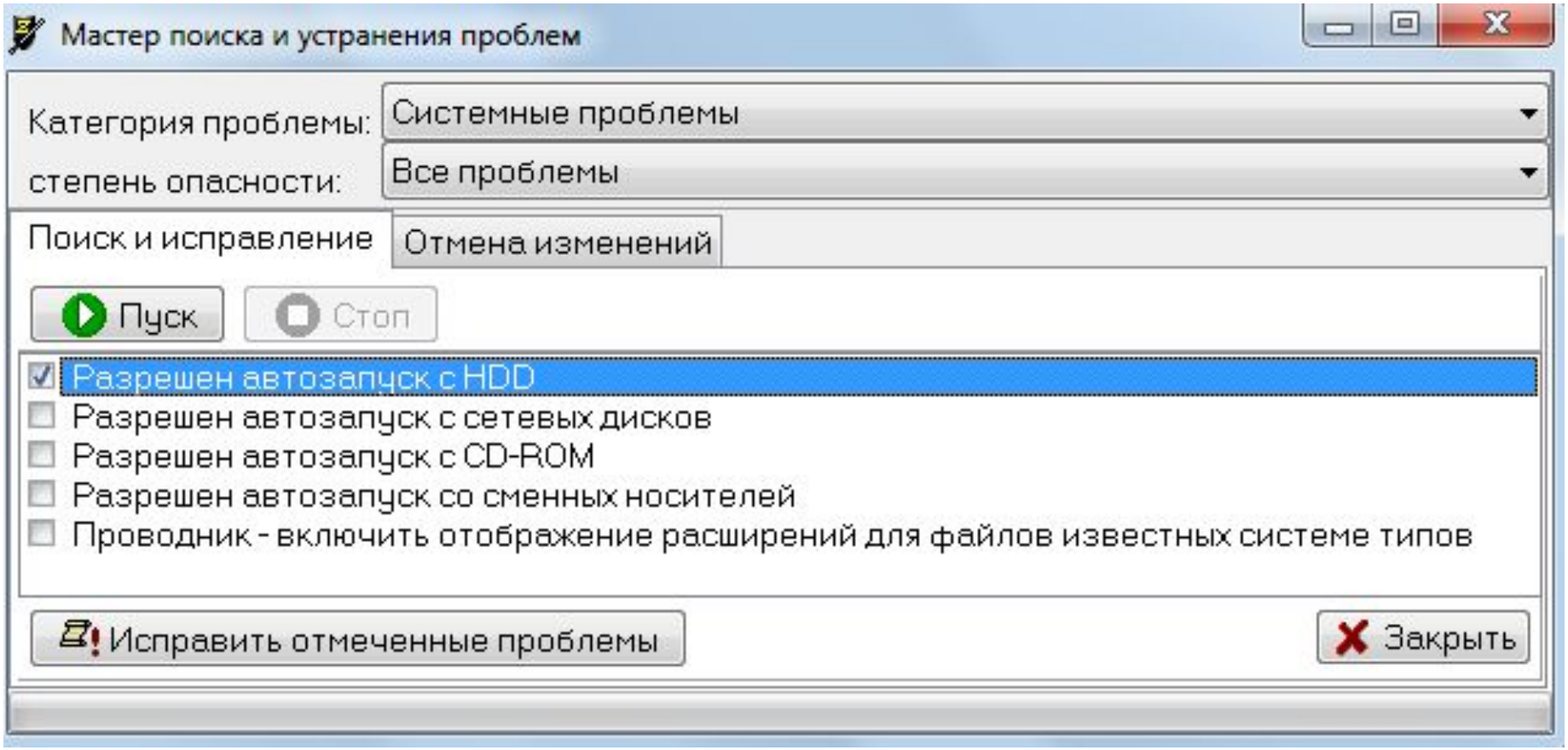


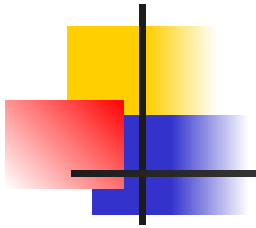
- Чтобы не разносить заразу, предварительно отключаем на «лечащем» компьютере автозапуск с HDD (да и с других типов носителей не мешало бы).
- Сделать это удобнее всего бесплатной утилитой AVZ, но саму проверку лучше выполнять чем-то другим.



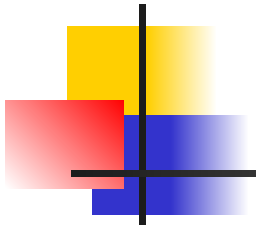
- Зайдите в меню «Файл», выберите «Мастер поиска и устранения проблем».
- Отметьте «Системные проблемы», «Все» и нажмите «Пуск».
- После этого отметьте пункт «Разрешён автозапуск с HDD» и нажмите «Исправить отмеченные проблемы».

Отключение автозапуска с помощью AVZ



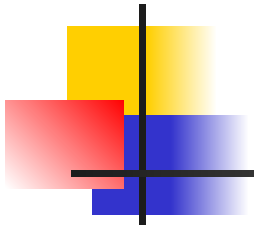


- Перед подключением заражённого винчестера стоит убедиться, что на компьютере запущен резидентный антивирусный мониторинг с адекватными настройками и есть свежие базы.



- Если разделы внешнего жёсткого диска не видны, зайдите в «Управление дисками».
- Для этого в окне «Пуск» -> «Выполнить» напишите diskmgmt.msc и затем нажмите {ENTER}.
- Разделам внешнего жёсткого диска должны быть назначены буквы.
- Их можно добавить вручную командой «изменить букву диска…».
- После этого проверьте внешний винчестер целиком.

- Для предотвращения повторного заражения следует установить любой антивирус с компонентом мониторинга в режиме реального времени и придерживаться общих правил безопасности.



Общие правила безопасности

Общие правила безопасности

- старайтесь работать из-под учётной записи с ограниченными правами;
- пользуйтесь альтернативными браузерами – большинство заражений происходит через Internet Explorer;
- отключайте Java-скрипты на неизвестных сайтах;

Общие правила безопасности

- отключите автозапуск со сменных носителей;
- устанавливайте программы, дополнения и обновления только с официальных сайтов разработчиков;
- всегда обращайте внимание на то, куда на самом деле ведёт предлагаемая ссылка;

Общие правила безопасности

- блокируйте нежелательные всплывающие окна с помощью дополнений для браузера или отдельных программ;
- своевременно устанавливайте обновления браузеров, общих и системных компонентов;
- выделите под систему отдельный дисковый раздел, а пользовательские файлы храните на другом.

Ресурсы

- http://www.computerra.ru/59610/trojan-windows-unlocking/
- http://support.kaspersky.ru/viruses/solutions?qid=208637133
- http://hardisoft.ru/soft/borba-s-programmami-vymogatelyami/
- http://kzncomputer.ru/articles/14-how-to-delete-the-banner
- http://mes-blog.com.ua/virusy/virus-blokiruet-windows.html
- http://todostep.ru/DelBanner.html