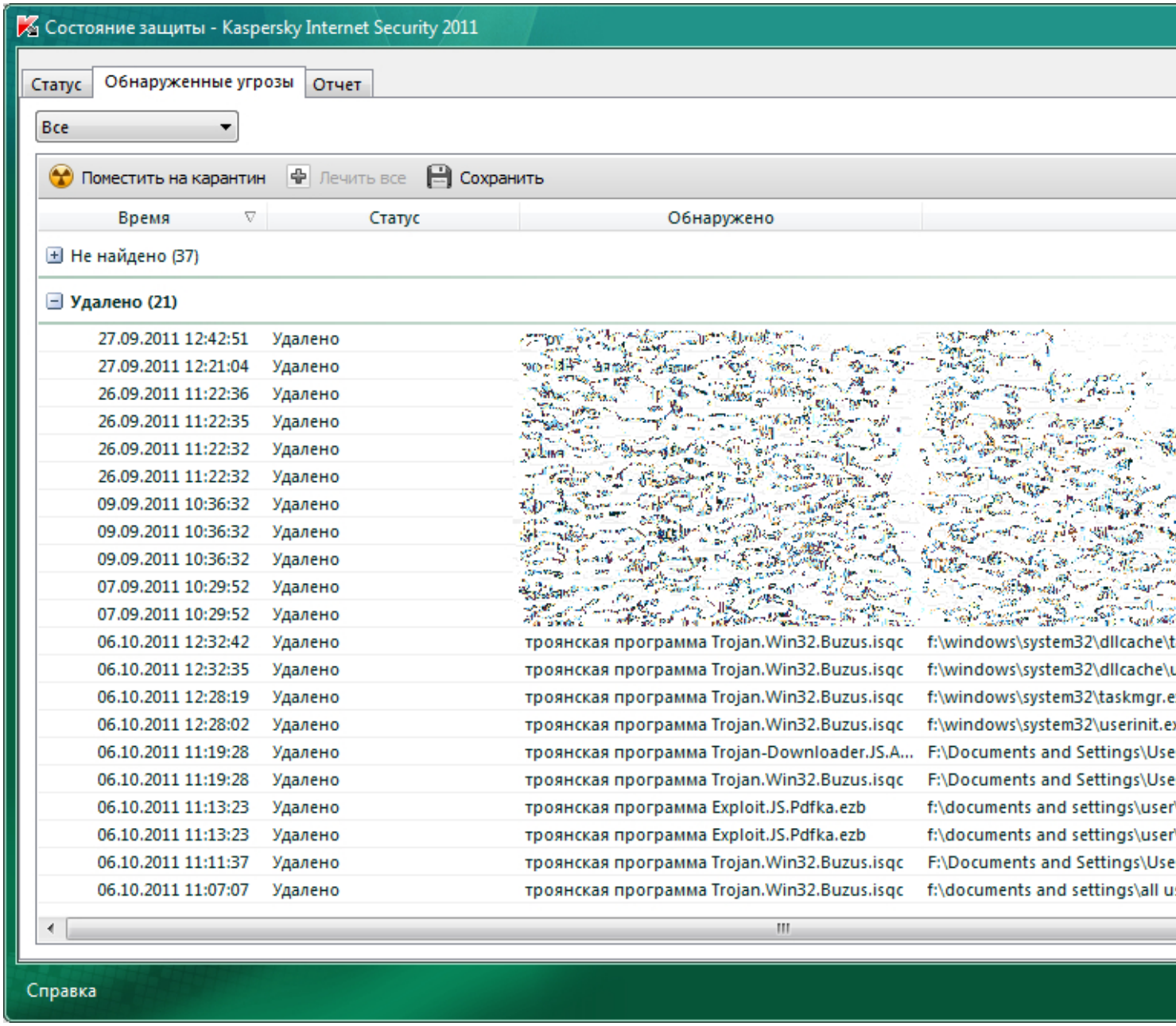
Очередной **блокер-вымогатель**. Проблема: после старта **Windows** XP всплывает баннер с требованием оплатить разблокировку.

Решение проблемы. Подключаем HDD к другому компьютеру с установленным KIS2011. Делаем проверку диска. Получаем результат:



Касперский идентифицирует системные файлы **taskmgr.exe** и **userinit.exe** как троянские программы
Buzus.isqc
а так же файлы
wpbt0.dll
и
22co6c32.exe
и удаляет их. Просмотрев лог можно предположить, что пользователь загрузил файл **calc[1].exe**, который создал файл со случайным именем **22co6c32.exe** и изменил системные файлы.

После проведенной процедуры запускаем Windows на вылеченом компьютере. Винда доходит до окна выбора пользователя. При попытке войти в учетную запись любого пользователя система завершает его сеанс. Это понятно - у нас не хватает системных файлов. Мы их подкидываем с рабочей копии винды. В реестре HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionWinlogon исправляем Shell (который был изменен зловредом на **22co6c32.exe**).

Скачать   **taskmgr.exe ** **userinit.exe**

Список статей: Разблокировать Windows