

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА  
МГУПС (МИИТ)  
ТАМБОВСКИЙ ЖЕЛЕЗНОДОРОЖНЫЙ ТЕХНИКУМ –  
Филиал федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Московский государственный университет путей сообщения Императора Николая II»

ПРЕЗЕНТАЦИЯ ПО ДИПЛОМНОМУ ПРОЕКТУ НА ТЕМУ:

# «ОПТИМИЗАЦИЯ МЕТОДОВ АНТИВИРУСНОЙ БЕЗОПАСНОСТИ ПРИ ПРОЕКТИРОВАНИИ СЕТЕЙ»

Специальность 09.02.02 «Компьютерные сети»

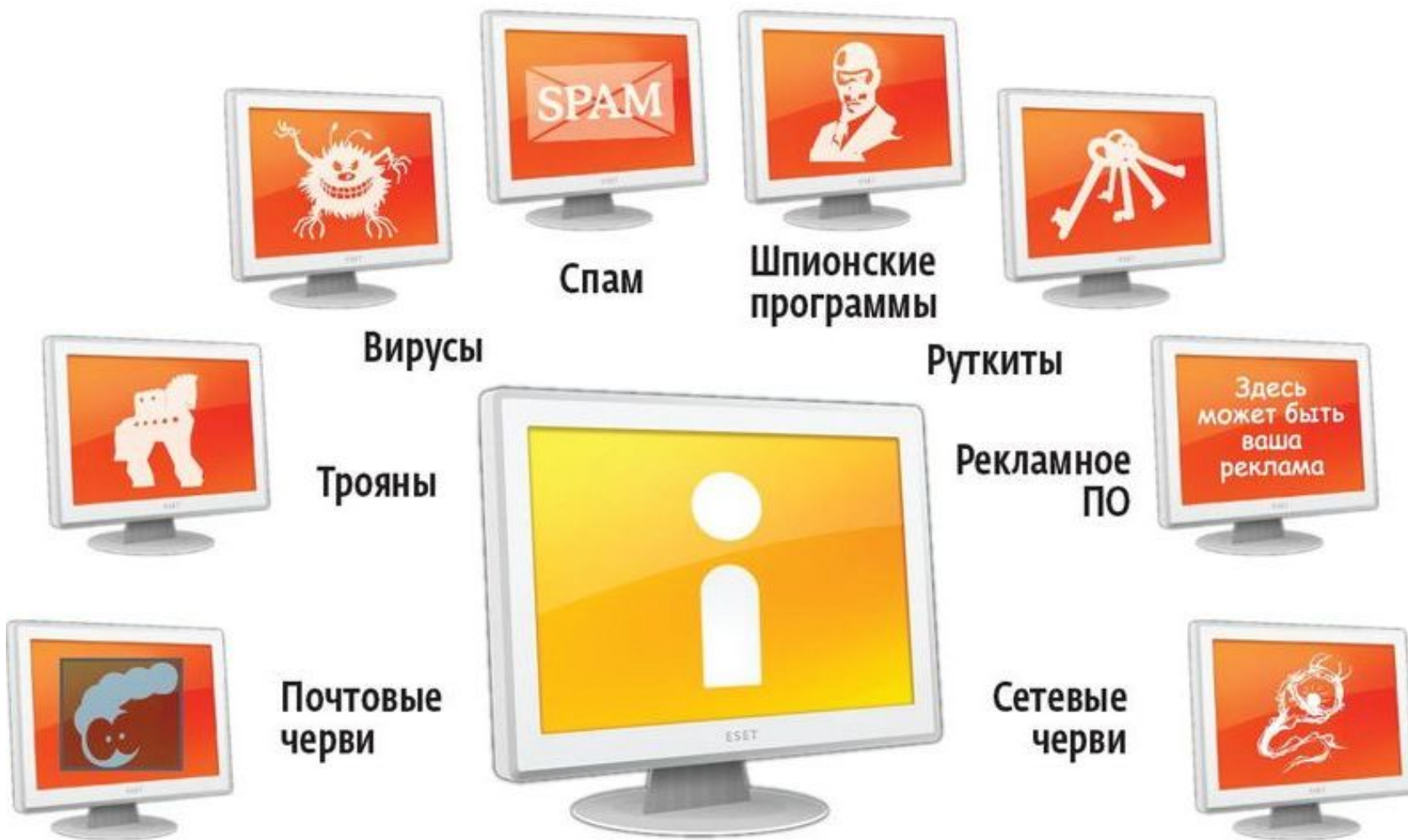
Студента: Ситникова Дмитрия Юрьевича гр. ТАКС – 411

Руководитель проекта: Раздольский В.Е

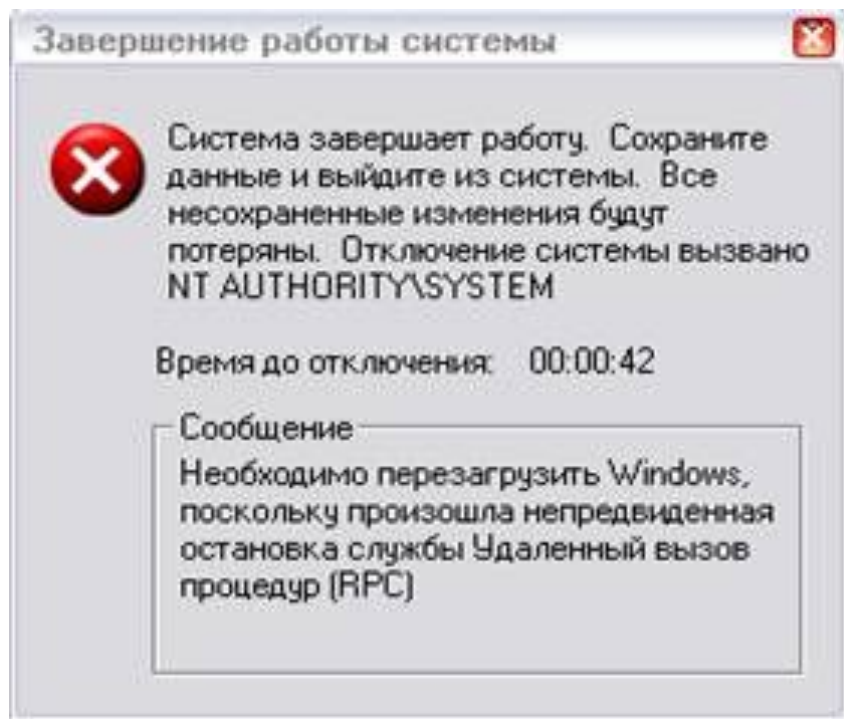
# Цели и задачи дипломного проекта

- Основной целью дипломного проекта является подбор антивирусных программ для реализации основных методов защиты информации и анализа её защищенности с учетом быстрого развития информационных технологий и новых угроз безопасности, а так же выработку соответствующих мер по предотвращению заражения компьютеров вирусными угрозами различных видов.
- Задачи, которые предстоит решить:
- 1. Провести исследования с целью выявления возможностей антивирусных программ обнаруживать вирусные угрозы, предотвращать заражение персональных компьютеров и удалять вредоносное программное обеспечение;
- 2. Проанализировать вирусные угрозы информационной безопасности;
- 3. Выработать меры по снижению риска заражения персональных компьютеров и защиты данных;
- Объектом исследования дипломной работы является антивирусные программы различных производителей и все возможные вирусные угрозы.

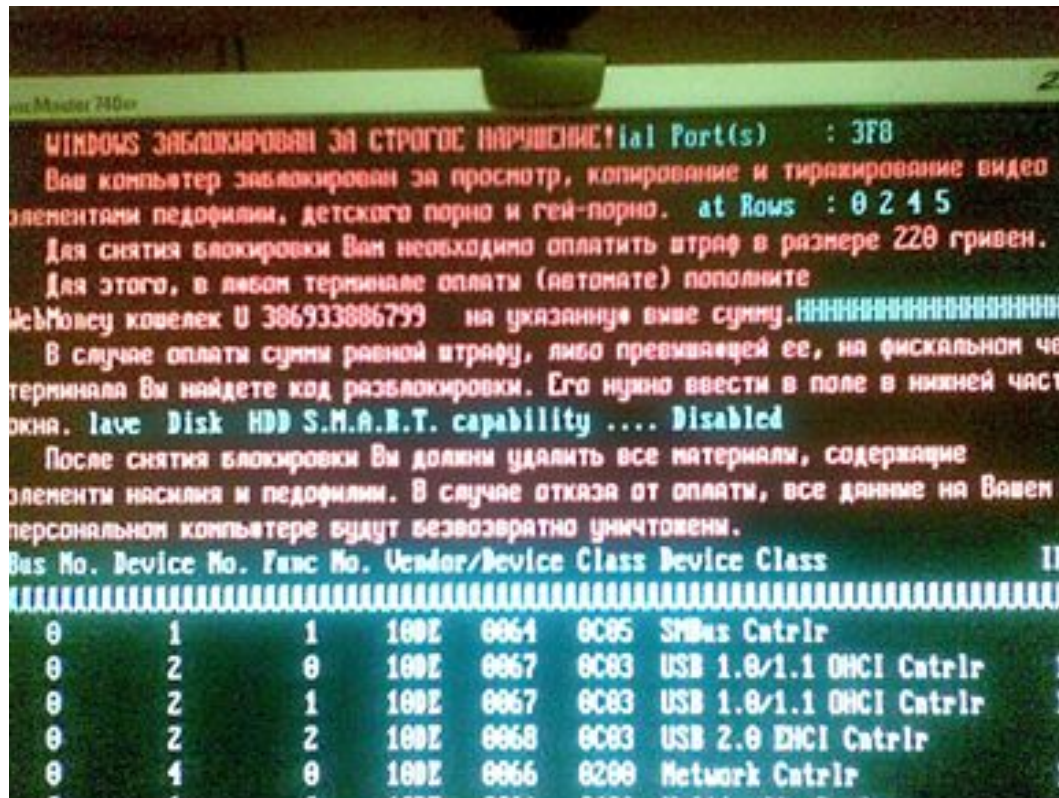
# Сетевые угрозы



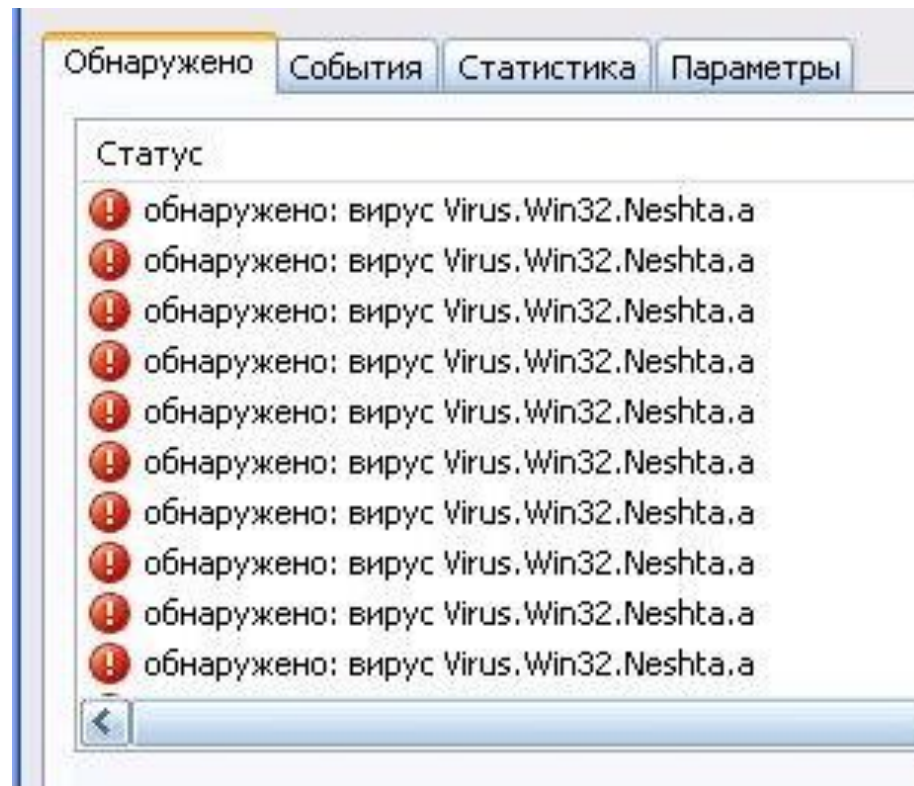
# Сообщение об ошибке – результат работы вируса Blaster



# Сообщение об ошибке – Вирус в загрузочном секторе Windows»

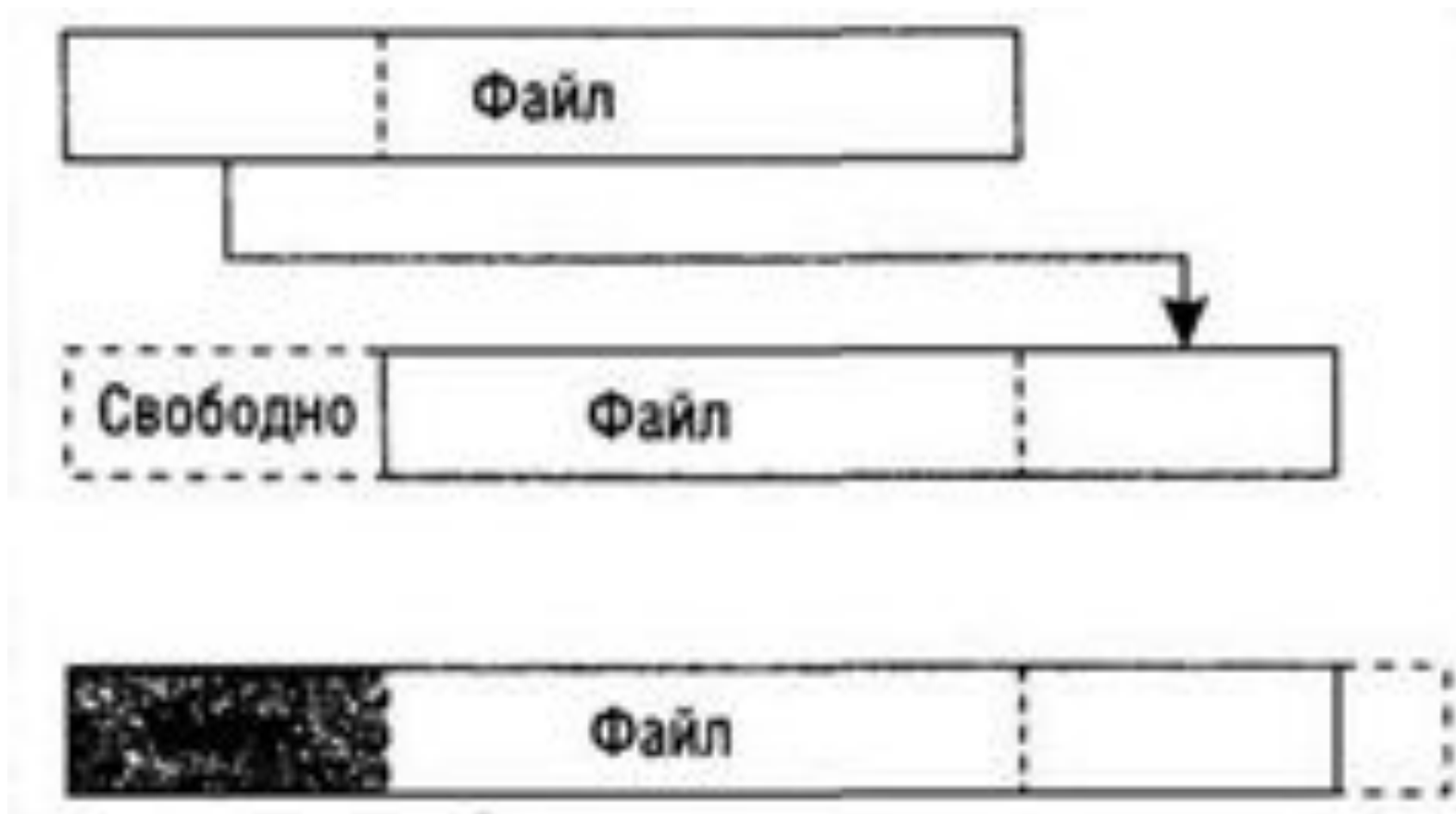


# Обнаружение файловых вирусов

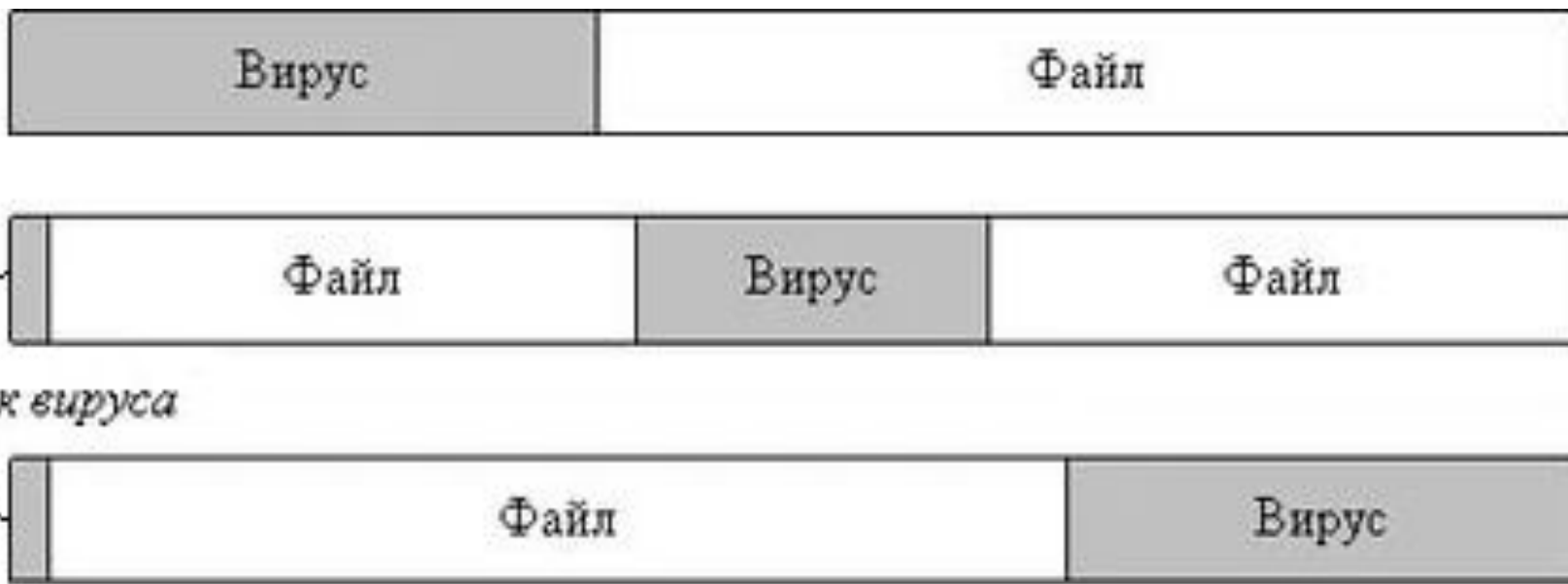




# Схема внедрение вируса в начало файла



# Схема внедрение вируса в файл





# Схема работы вирусов без точки входа



# Сообщение об ошибке – вирусная-ссылка.



## The site ahead contains malware

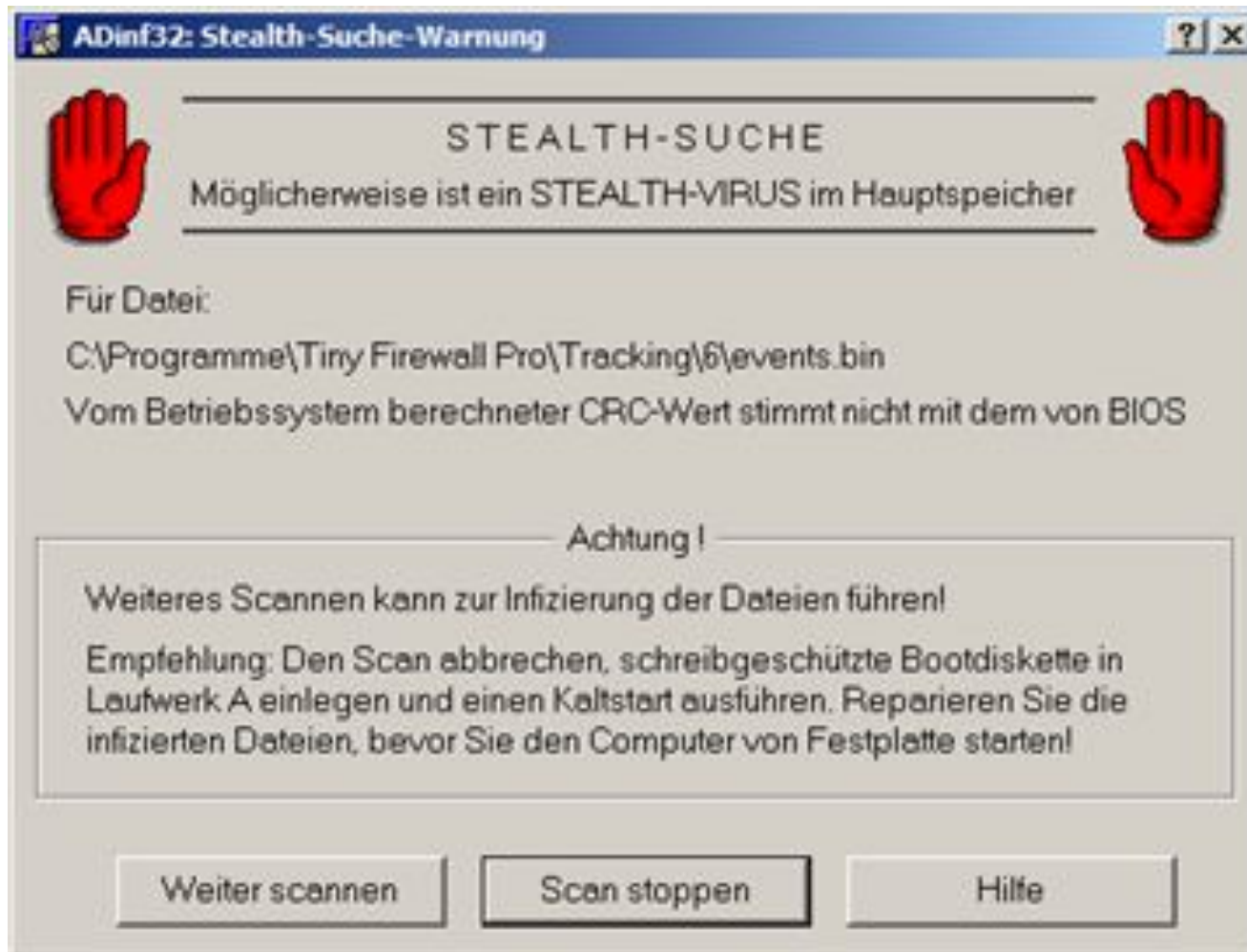
Attackers currently on [soaksoak.ru](#) might attempt to install dangerous programs on your Mac that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

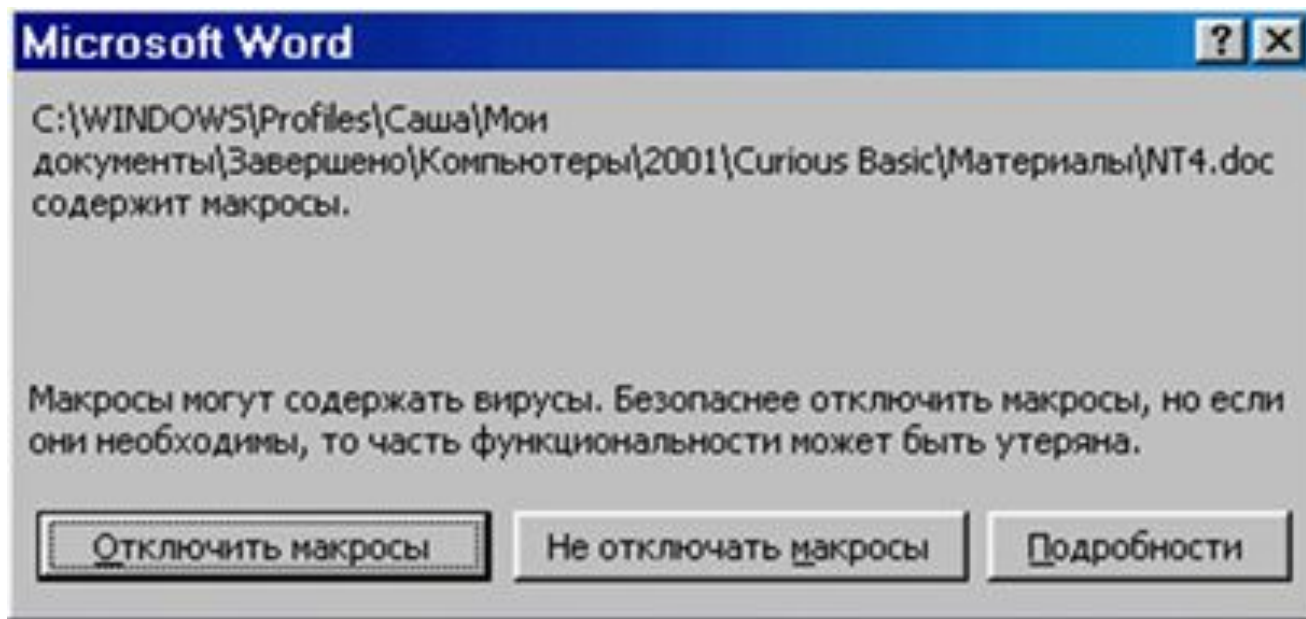
[Details](#)

[Back to safety](#)

# Сообщение об ошибке – обнаружение стелс-вируса



# Сообщение об угрозе заражения макровирусом

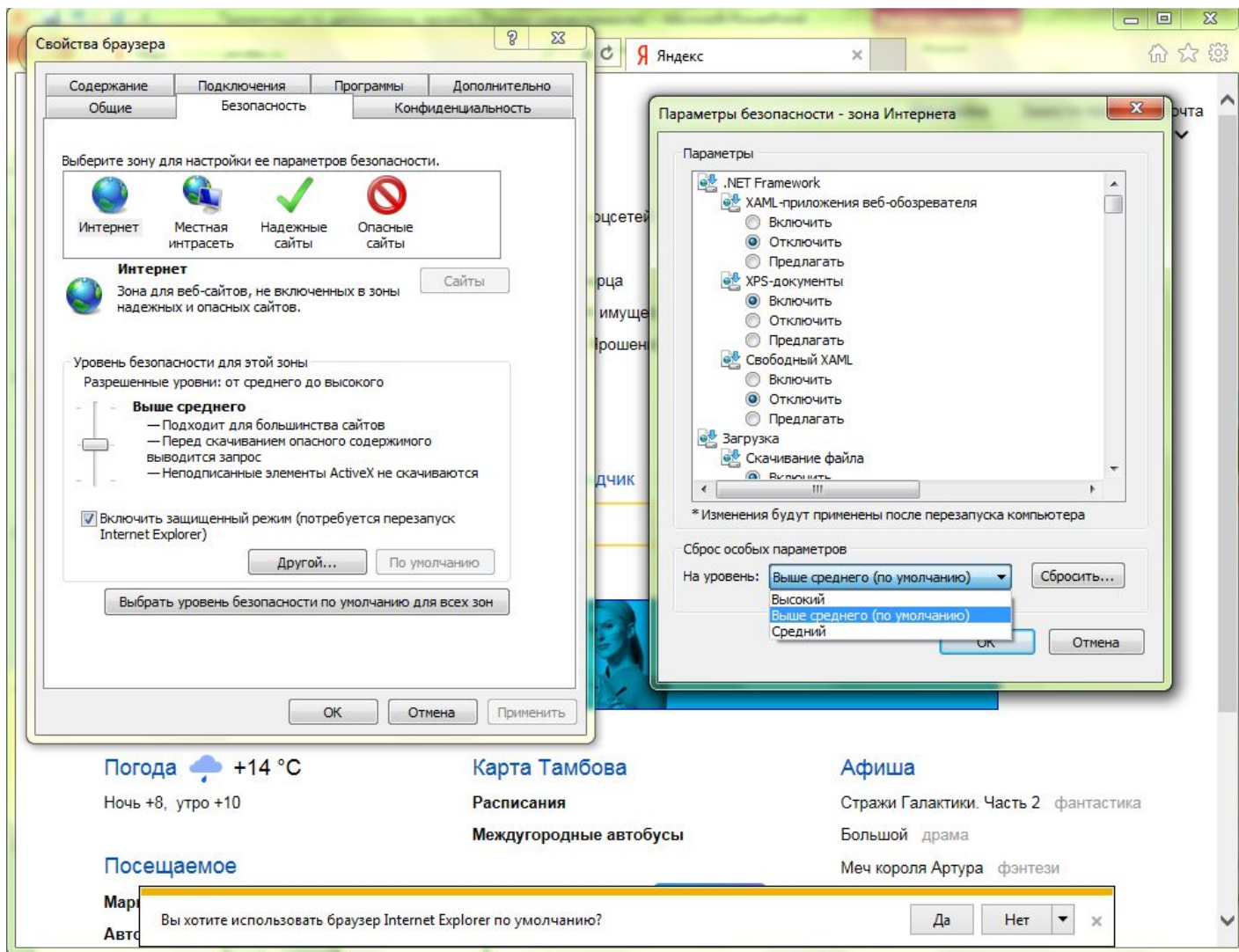


# Программный код скрипт-вируса

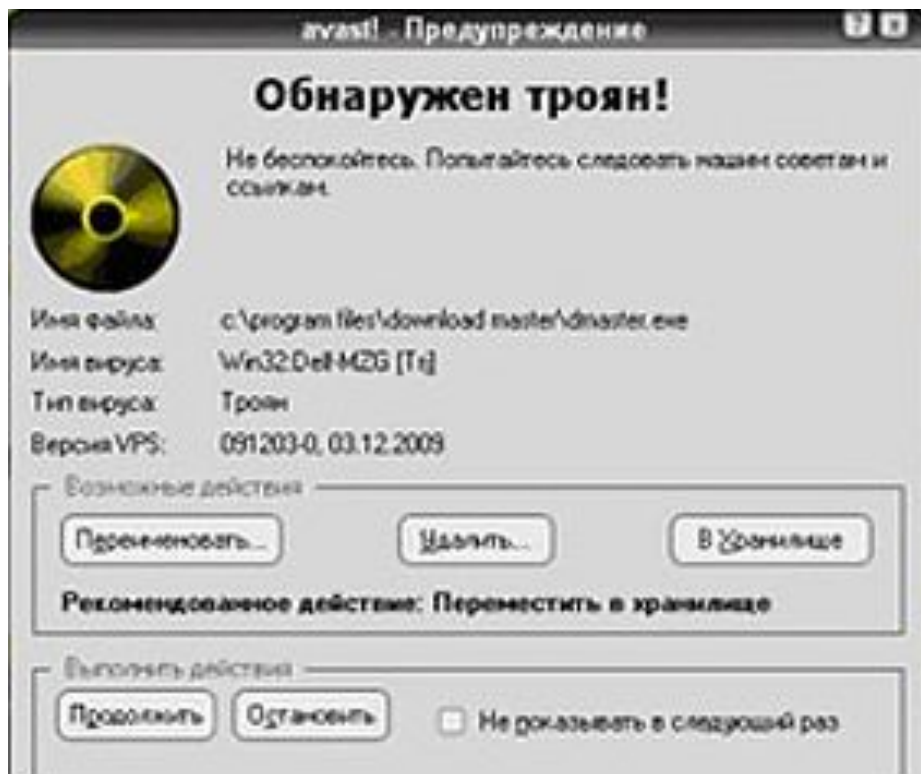
```
Windows PowerShell
C:\Windows\system32\cmd.exe 328a95 Reportada como Limpio.
C:\Windows\system32\conhost.exe 318e9119d8a1cf4f1da89780796533d81 Reportada como Limpio.
C:\Program Files\OpenDNS\DNSCrypt\OpenDNSCryptService.exe 6f865de868776ec845f79cc965643626 Reportada como Limpio.
C:\Program Files\OpenDNS\DNSCrypt\dnscrypt-proxy.exe 5188142eaf978a6631f92795a303180 No se encuentra en la base de datos de VT.
https://www.virustotal.com/file/289f87266217999c90408f62b59dafaf4c42d81432ebc1d5bab0f3f961764329/analysis/1362913061/
C:\Windows\system32\conhost.exe 318e9119d8a1cf4f1da89780796533d81 Reportada como Limpio.
C:\Program Files\NVIDIA Corporation\NVIDIA Update Core\dacemonu.exe 81e08b8fa53ed15dc784fa34b44b80f Reportada como Limpio.
C:\Windows\system32\cmd.exe ad7b9c14883a52ba532fba5748342b98 Reportada como Limpio.
C:\Windows\system32\WINED3D.dll 326c7f76a29877a872aa7726e91c1c17 Reportada como Limpio.
C:\Program Files\Foxit Software\Foxit Reader\Foxit Reader.exe 4798cd7942843e7f24bb4321b3a13f46 Reportada como Limpio.
C:\Windows\system32\scpfilter.dll 088cf536388f179802f2a4246f812225d Reportada como Limpio.
C:\Windows\system32\SearchProtocolHost.exe 51ac87f6c5252857e4862843e36a6701 Reportada como Limpio.
C:\Windows\system32\PCSShells.dll ac4277866738258952c86f466a883e8 Reportada como Limpio.
C:\Windows\system32\scpfilter.dll 4367c7c82838de812c6486581a7611 Reportada como Limpio.
C:\Windows\system32\scpfilter.dll 8be9d92c4b2f2ba89185bab2afcf16 Reportada como Limpio.
C:\Windows\hh.exe 9b788bc78471a4881d8c91941f16f279 Reportada como Limpio.
C:\Windows\System32\ntos.dll 85408a7384726565f1254dc438b43c42 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\Firefox.exe bf2f272e12a4b44f47f2788f514e865 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\Firefox.exe 57ec459e4243881d48f1d34356f7cafc1 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozglue.dll 8a90f5d9f6552f4f3c822487f4e23f9f Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll a8bc87252226adaffefc6b5b5dbcc807f Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll 81e73148094f504a146c17d3c4b6276c Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll 8c23d9ab3a688a6f71a3c655c4fcf73 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\glue.dll bd79e72c84d7098e8d4c7613481437c Reportada como Limpio.
C:\Program Files\Mozilla Firefox\glue.dll a4f52abd5a3a07783a3ad79c6d92568a Reportada como Limpio.
C:\Program Files\Mozilla Firefox\winutil.dll 0488801d7807277474681385b8c7cadda Reportada como Limpio.
C:\Program Files\Mozilla Firefox\winutil.dll 4a88796a418575e2b3af88972a4ab989 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\winutil.dll a79e881fa1376ad548044baad6a824 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\winutil.dll 8a802104133543f79c87ab8455486e85 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozglue.dll a2af12f6dd82f7c25f08f72cd7776c8 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozalloc.dll a7c1f254d94c458ade17e64727e6649 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozalloc.dll 83922128e812b53ff588cc8410a681e Reportada como Limpio.
C:\Program Files\Mozilla Firefox\winutil.dll 9fa6e8d24c4ab8e85c92271d82faa1 Reportada como Limpio.
C:\Windows\system32\cmd.exe 7867a88536f229e7223140972a2874b Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mpcom.dll 18965ec91ba8ab48cc47174cfff4 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\components\browsercomps.dll 47841291844018701aef852a53827668 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozalloc.dll 6f89e374cc912745efedd4488cb8a5 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozalloc.dll ba874c812651d88852a9587f70f636d1 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\freebl.dll d388812a7e8ca6e83f1c2c13339f94 Reportada como Limpio.
C:\Windows\system32\Nls\Phone1.dll 2e873242258918e8d888a982a5ca1f Reportada como Limpio.
C:\Windows\system32\Nls\UnicodeProvider.dll 8fcd13c5a815d89f8ca1fd39d3118b7 Reportada como Limpio.
C:\Windows\system32\Nls\UnicodeProvider.dll 15fe887a23618f18fa4b2d26c728baf Reportada como Limpio.
C:\Windows\system32\Nls\UnicodeProvider.dll 126b795d8756fe2042334418ae1a6df Reportada como Limpio.
C:\Windows\system32\Nls\UnicodeProvider.dll 6e6412a7e015a3aa2a27b9cc12537 Reportada como Limpio.
C:\Windows\system32\Nls\UnicodeProvider.dll 7d34af78a786238cc24edf8cabf87ab Reportada como Limpio.
C:\Windows\system32\Nls\UnicodeProvider.dll 46a8a9274d075a2c38825c4968875a Reportada como Limpio.
C:\Windows\system32\Nls\UnicodeProvider.dll aba457bf7c7c8b6e13882f1e881549df Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozalloc.dll 84a8894f21711c838d915dc33cc2a7d Reportada como Limpio.
C:\Windows\system32\Facility.dll a2631c4465380622676f7716f3924a943 Reportada como Limpio.
C:\Program Files\NVIDIA Corporation\3D Vision\Nv3DVisionStreaming.dll 9548f5c58a995f339858a32cd13ad4f No se encuentra en la base de datos de VT.
C:\Program Files\NVIDIA Corporation\3D Vision\Nv3DVision.dll 6f04ab8a812855acha9aalcd85ab242 No se encuentra en la base de datos de VT.
C:\Program Files\NVIDIA Corporation\3D Vision\NvSCPAPI.dll f187564dc311d8c1a1742e5e1858abfe No se encuentra en la base de datos de VT.
C:\Program Files\Classilla\Classilla.exe 8888a64967bcbf9ac7021538e5a3c2 Reportada como Limpio.
```



# Настройка уровня безопасности Internet Explorer

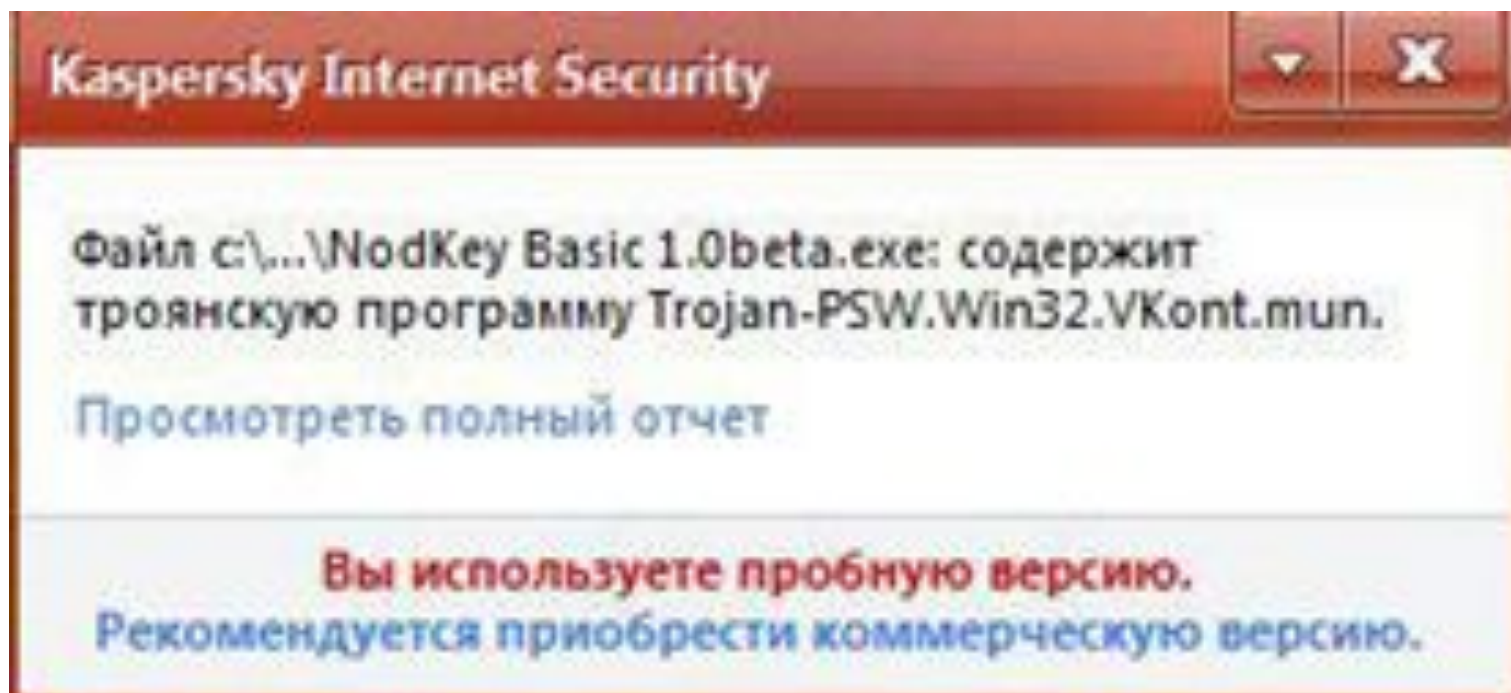


# Сообщение об обнаружении угрозы «Троян»





# Сообщение об обнаружении угрозы «Trojan-PSW»



# Сообщение об обнаружении угрозы «Trojan- Clicker»

## ДОСТУП ЗАПРЕЩЕН

Запрашиваемый URL-адрес не может быть предоставлен

**В запрашиваемом объекте по URL-адресу:**

<http://www.award.kz/forum/login.php>

**Обнаружена угроза:**

объект заражен [Trojan-Clicker.HTML.IFrame.qt](#)

Пожалуйста, обратитесь к вашему провайдеру, если вы считаете это сообщение ошибочным.

# Сообщение об обнаружении «Trojan-Downloader»



# Сообщение об обнаружении «Trojan- Dropper»



# Архивная бомба





# Схема заражения компьютеров по средствам электронной почты



# Сообщение об обнаружении вируса «Klez»





# Письмо с IRC-Worm вирусом



756918030- i64ev - og400

РамЗнакр/омстблева <bezotveta@dating.rambler.ru>

14 мая, 3:22 1 файл



Письмо попало в папку «Спам», потому что оно похоже на сообщения, которые ранее были отфильтрованы нашей системой как спам. [Подробнее](#)

Жду там ваш поиск , если заинтересую <http://www.google.com/#tbsajop=1&q=4fr971fs4s7> > Жду там ответ

Все файлы проверены, вирусов нет

1 файл



pOe1aM4G3x.exe

525 КБ [Посмотреть](#) [Скачать](#) [Редактировать](#) [В Облако](#)

# Сообщение об ошибке при запуске «Червя».



# Сообщение об сетевой атаке



**Внимание! Ваш компьютер был атакован.**

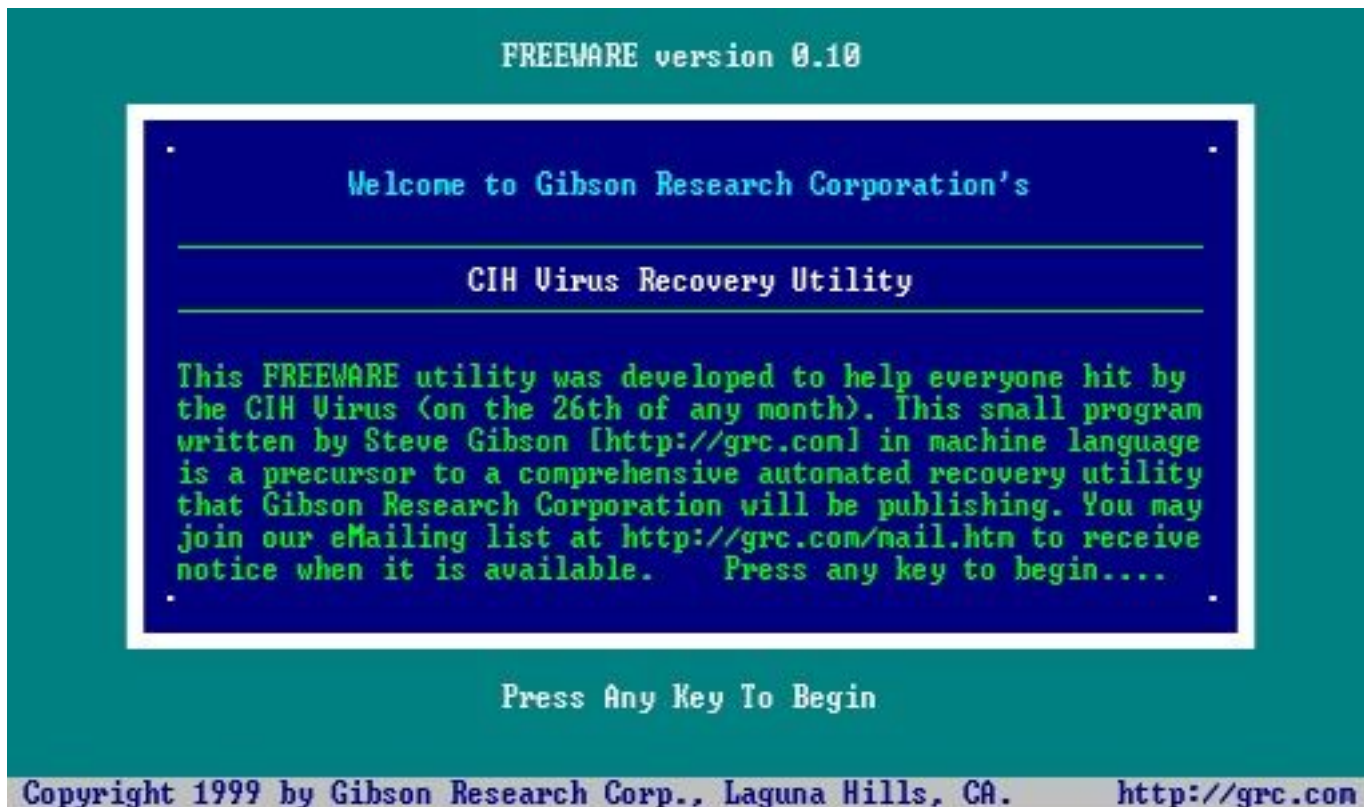
Сетевая атака **not-an-attack:KL-Test-Packet** с адреса 172.16.1.58 была успешно отражена.

# Сообщение об сетевых атаках и их блокировка

The screenshot displays the Kaspersky Internet Security 2013 interface. A notification window is open, stating: "Сетевая атака DoS.Generic.SYNFlood: TCP от 77.34.160.210 на локальный порт 29837. Заблокировано. Атакующий компьютер заблокирован." Below the notification is a "Подробнее..." link. The main window shows a log of events for the period 01.01.2013 - 31.12.2013. The log table contains the following data:

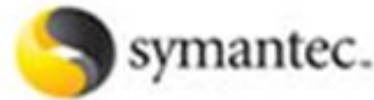
Событие	Время	Путь
локаль... Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38	
на лока... Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38	
на локаль... Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38	
✓ TCP от 225.239.130.214 на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 210.89.43.41 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 179.187.1.21 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 88.248.115.31 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 213.80.163.17 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 85.108.57.125 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 95.189.47.4 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 201.2.248.2 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 78.139.233.36 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 31.47.160.112 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 86.62.110.17 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 91.224.217.114 на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 95.154.79.50 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 109.191.39.16 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 212.87.229.94 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 77.243.99.24 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 78.169.218.151 на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 94.73.250.91 на локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 46.159.243.152 на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 189.100.106.18 на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
Защита от сетевых атак	Задача запущена	06.09.2013 15:31:36

# Программа для написания КОМПЬЮТЕРНЫХ ВИРУСОВ

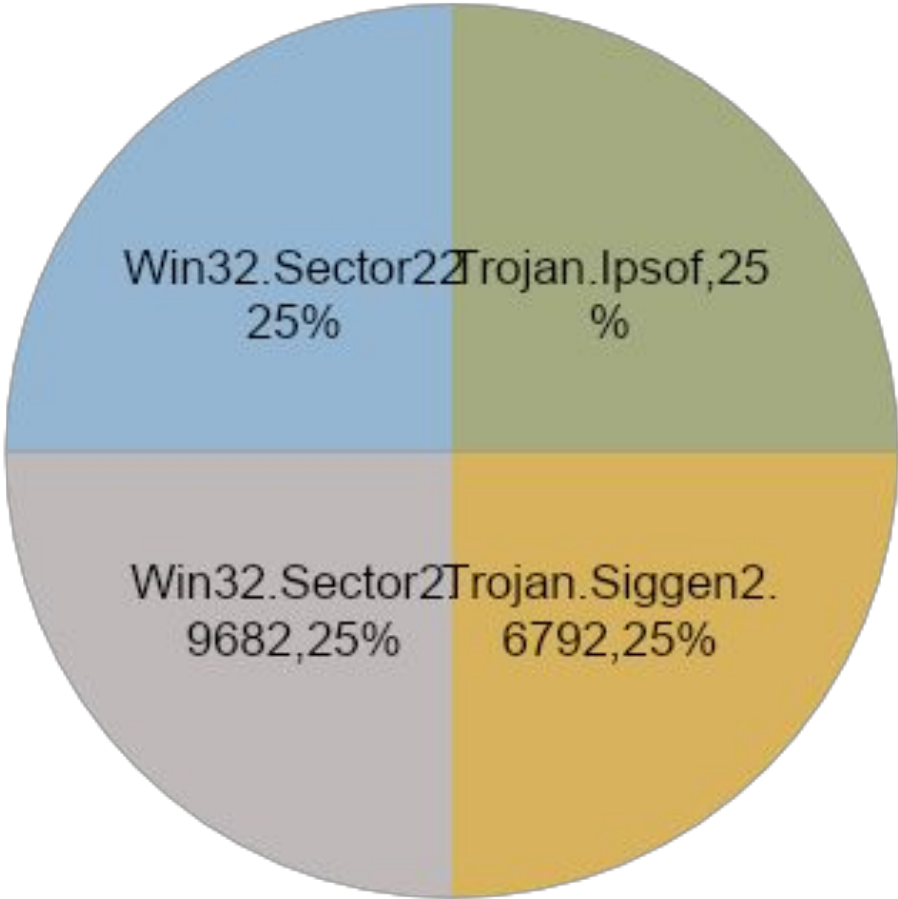


# Антивирусные программы принимавшие участие в тесте

- AVAST Antivirus
- AVG AntiVirus Free
- PC Tools Antivirus
- ESET NOD32 Antivirus
- Norton Antivirus

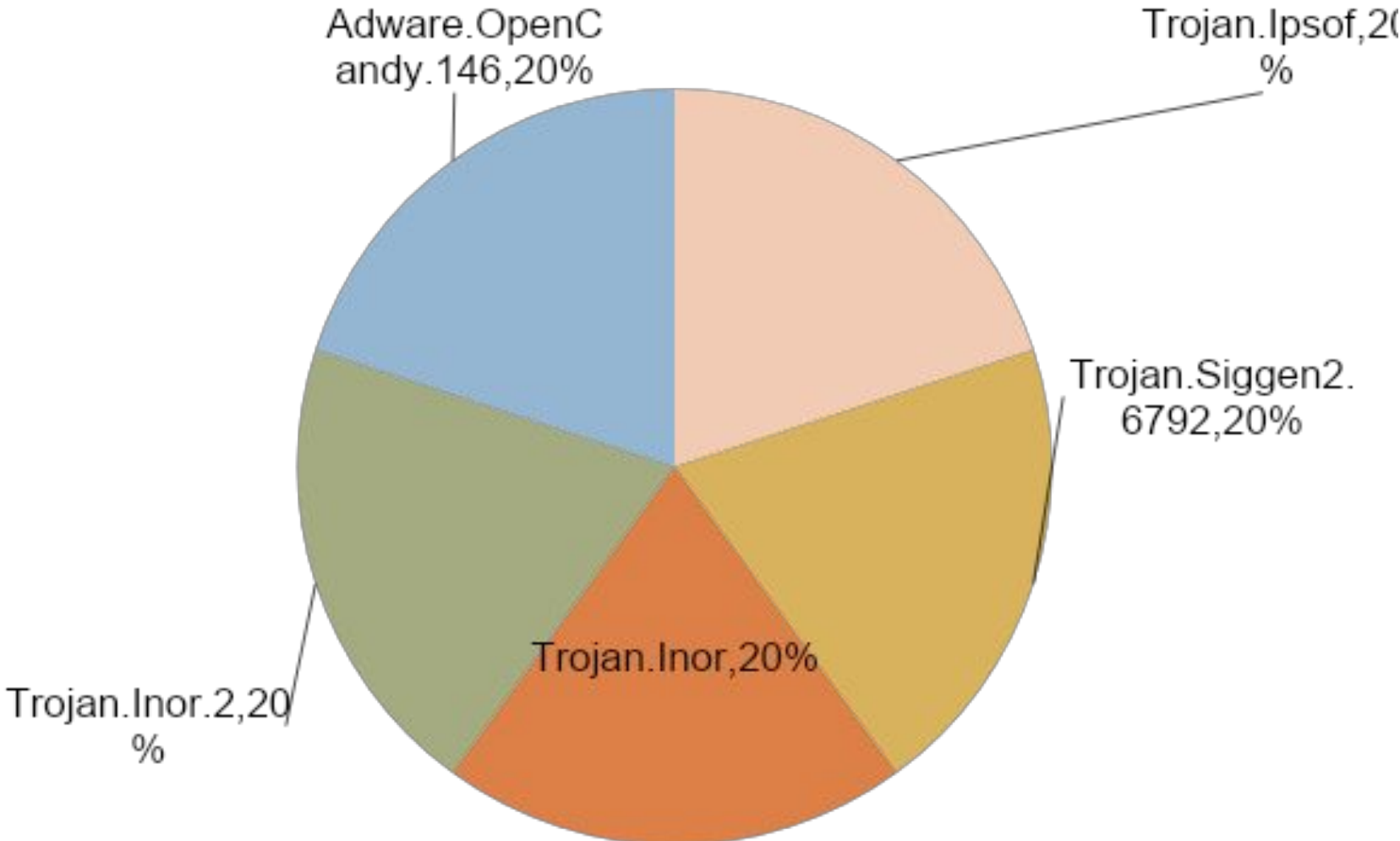


# AVAST Antivirus

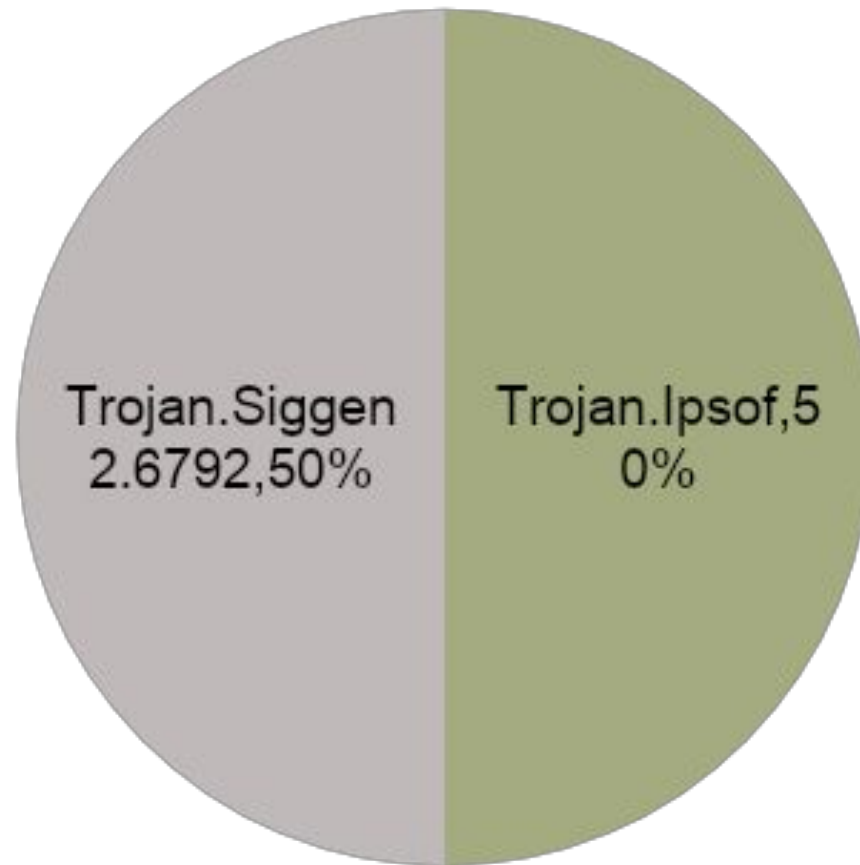




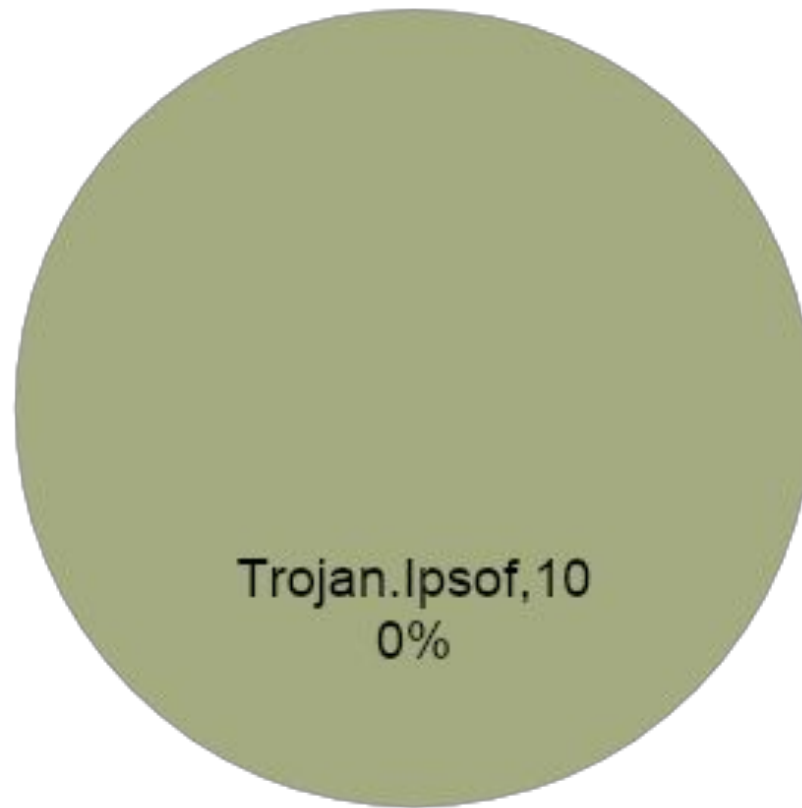
# AVG AntiVirus Free



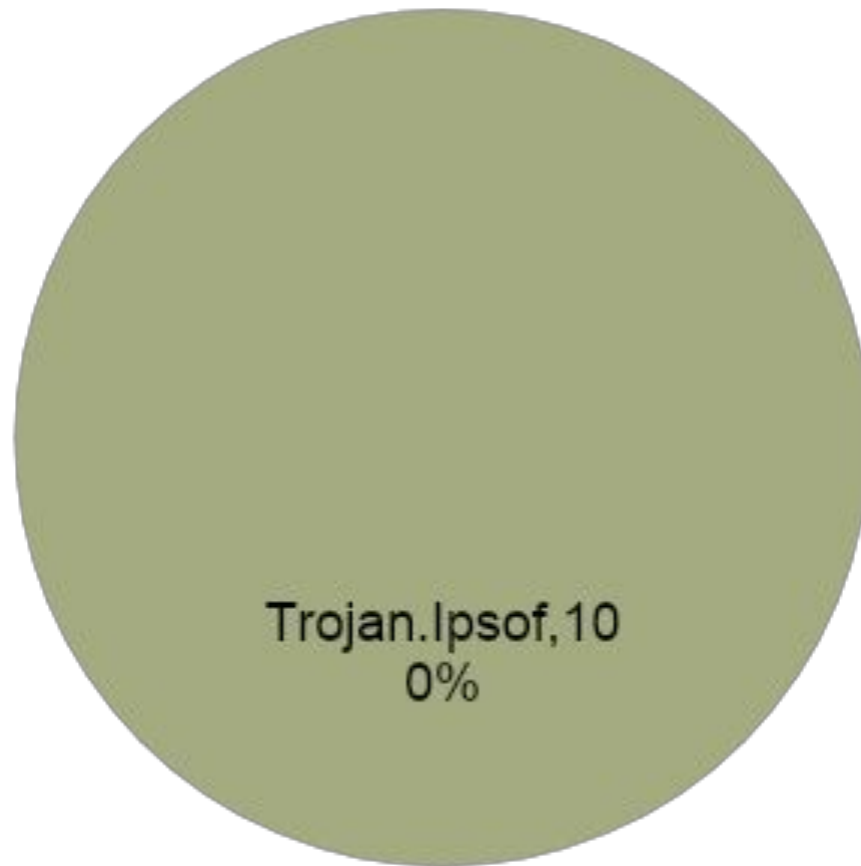
# PC Tools Antivirus



# ESET NOD32 Antivirus



# Norton Antivirus





# Dr.Web Enterprise Server



# Затраты организации не использующей антивирусное ПО

- ❑ Вирусы выводящие из строя комплектующие компьютера:
- ❑ Средняя цена материнской платы от 3000 руб. до 8000 руб.
- ❑ Средняя цена блока питания от 700 руб. до 1200 руб.
- ❑ Средняя цена жесткого диска от 2500 руб. до 9500 руб.



# Затраты организации не использующей антивирусное ПО

- Вирусы удаляющие разделы на жестком диске:
- Средняя цена за программное восстановление разделов с жестких дисков от 1500 руб.
  
- Вирусы удаляющие или повреждающие файлы:
- Средняя цена за восстановление данных после действий вирусов и троянов от 3000 руб.

# Затраты организации не использующей антивирусное ПО

- Вирусы шифрующие файлы:
- Средняя цена за расшифровку файлов после действия вируса от 4500 руб.

# Затраты на антивирусное ПО

№	Антивирус	Период	Количество	Цена	Скидка
1	Kaspersky	1 год	10 ПК	28 203,96 руб.	
2	Dr.Web	1 год	10 ПК	14 900,00 руб.	65%
3	Avast	1 год	10 ПК	7 992,00 руб.	13%
4	AVG	1 год	10 ПК	14 767,20 руб.	20%
5	ESET NOD32	1 год	10 ПК	12 208,00 руб.	
6	Norton	1 год	10 ПК	2 599,00 руб.	18%

# Рекомендации при использовании антивирусных программ

- При работе с внешними носителями информации обязательно проверяйте их антивирусной программой.
- Ни в коем случае не запускайте внезапно появившиеся на Рабочем столе значки.
- При получении из Интернета или локальной сети файлов проверьте их надежной антивирусной программой.
- Время от времени нужно полностью сканировать компьютер на наличие вирусов с помощью хорошей антивирусной

# Заключение

- На мой взгляд, достаточно установить на компьютере программу Dr.Web. Она не требовательна к ресурсам в отличие от Антивируса Касперского и Norton Antivirus'а. Антивирусные базы пополняются довольно часто.
- Единственный цивилизованный способ защиты от вирусов я вижу в соблюдении профилактических мер предосторожности при работе за компьютером.

# Спасибо за внимание!



# КОНЕЦ