

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»

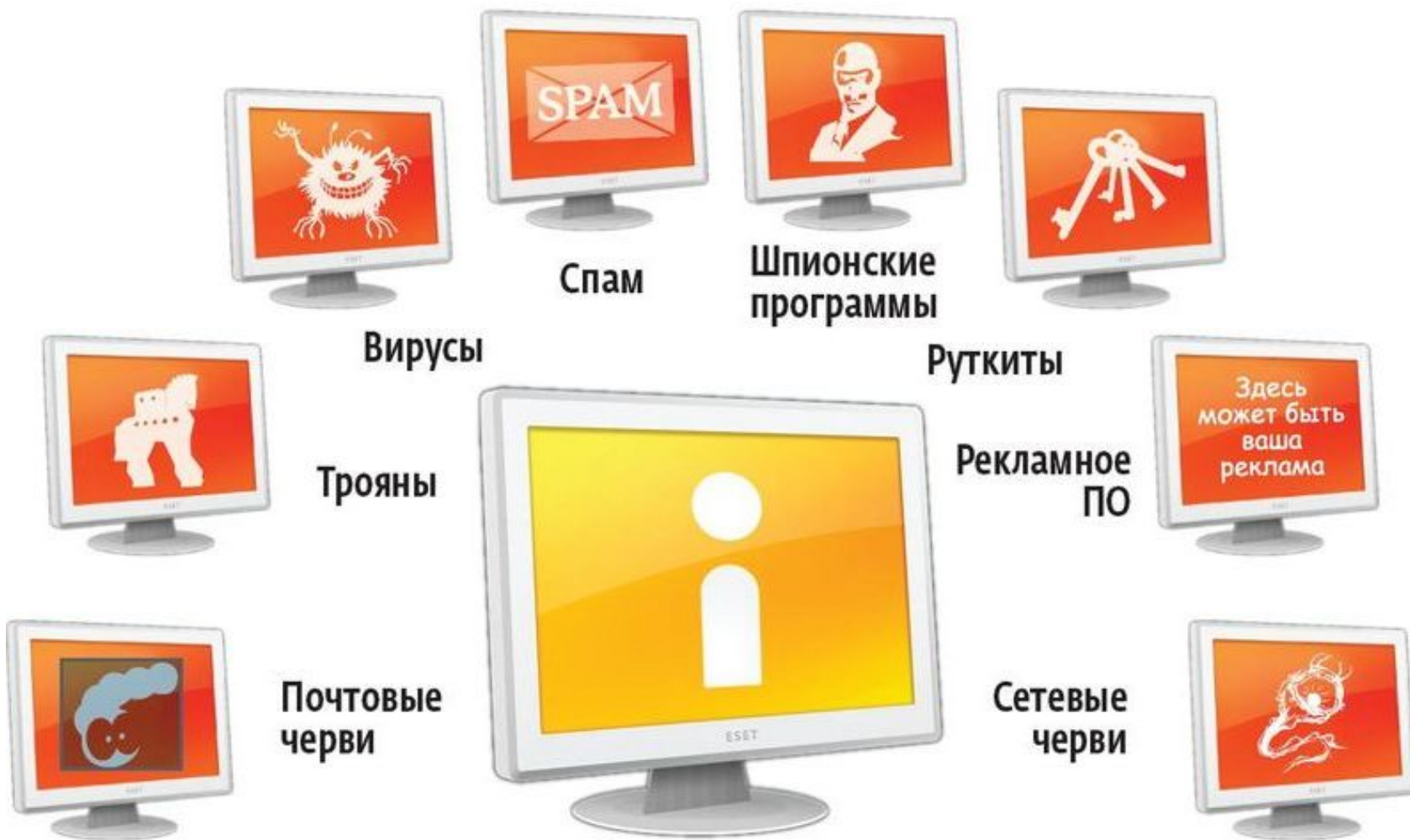
Студента: Ситникова Дмитрия Юрьевича гр. ТАКС – 411

Руководитель проекта: Раздольский В.Е

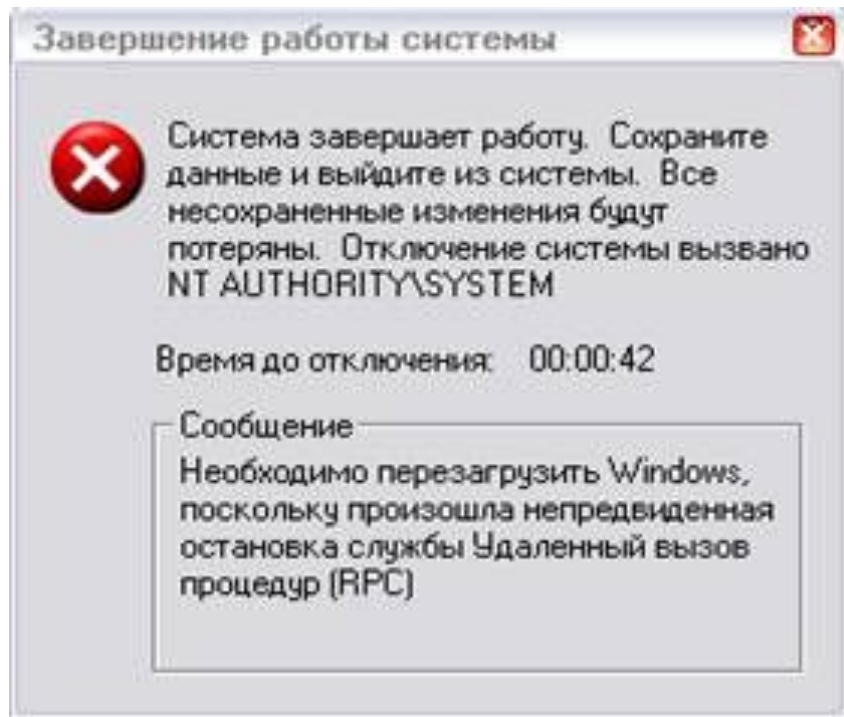
Цели и задачи дипломного проекта

- 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.

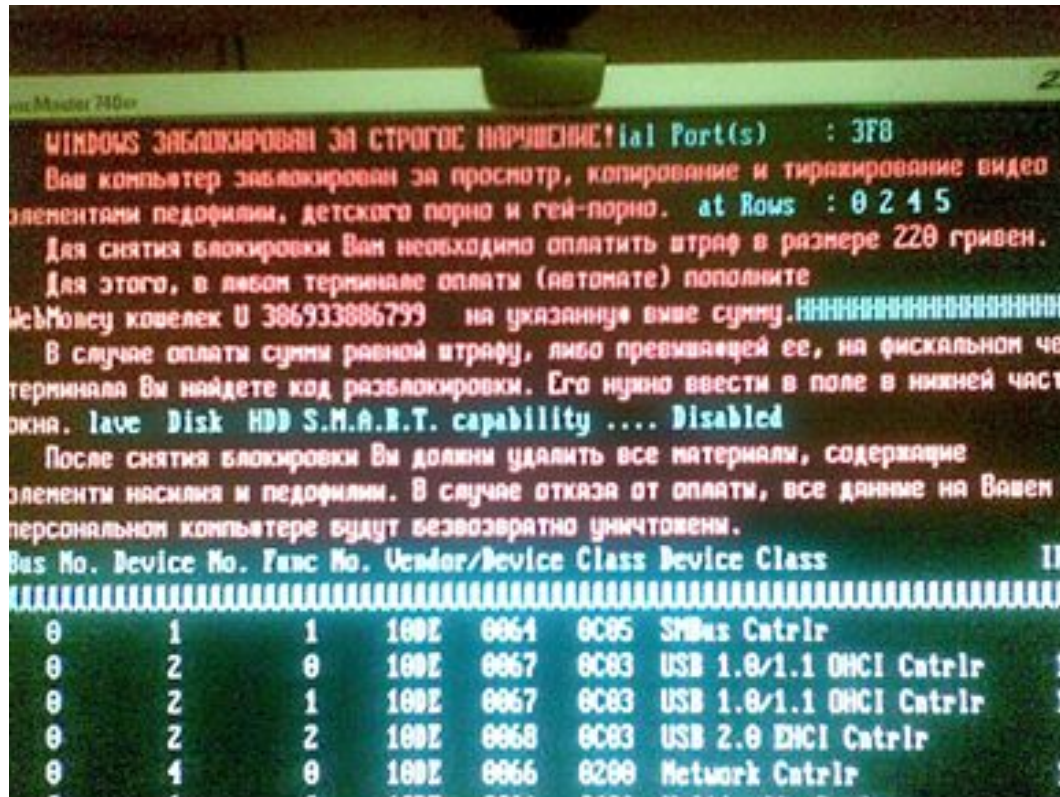
Сетевые угрозы



Сообщение об ошибке – результат работы вируса Blaster



Сообщение об ошибке – вирус в загрузочном секторе Windows»



```

Microsoft Windows [Версия 6.0.6002.18000] Copyright (c) 2009 Microsoft Corporation. Все права защищены.
Microsoft Windows [Версия 6.0.6002.18000] Copyright (c) 2009 Microsoft Corporation. Все права защищены.
Microsoft Windows [Версия 6.0.6002.18000] Copyright (c) 2009 Microsoft Corporation. Все права защищены.

МikrowMS заблокирован за строгое нарушение!
Ваш компьютер заблокирован за просмотр, копирование и тиражирование видео элементов педофилии, детского порно и гей-порно.
Для снятия блокировки Вам необходимо оплатить штраф в размере 220 гривен.
Для этого, в любом терминале оплаты (автомате) пополните
McMONEY кошелек U 306933886799 на указанную выше сумму.
В случае оплаты суммы равной штрафу, либо превышающей ее, на фискальном чеке терминала Вы найдете код разблокировки. Его нужно ввести в поле в нижней части окна.
После снятия блокировки Вы должны удалить все материалы, содержащие элементы насилия и педофилии. В случае отказа от оплаты, все данные на Вашем персональном компьютере будут безвозвратно уничтожены.

Windows 7 Home Premium
Intel Core i5-750 2.66GHz
8GB RAM
Intel HD Graphics 3000
Hard Disk: 500GB
DVD Burner
Mouse
Keyboard

Диск: SATA Hard Disk 7200rpm
Состояние:良好
См. также журнал событий.

Microsoft Windows [Версия 6.0.6002.18000] Copyright (c) 2009 Microsoft Corporation. Все права защищены.
Microsoft Windows [Версия 6.0.6002.18000] Copyright (c) 2009 Microsoft Corporation. Все права защищены.
Microsoft Windows [Версия 6.0.6002.18000] Copyright (c) 2009 Microsoft Corporation. Все права защищены.

Bus No. Device No. Func No. Vendor/Device Class Device Class
=====
0 1 1 100E 0064 0C85 SMBus Contrlr
0 2 0 100E 0067 0C83 USB 1.0/1.1 OHCI Contrlr
0 2 1 100E 0067 0C83 USB 1.0/1.1 OHCI Contrlr
0 2 2 100E 0068 0C83 USB 2.0 OHCI Contrlr
0 4 0 100E 0066 8200 Network Contrlr

```

Обнаружение файловых вирусов

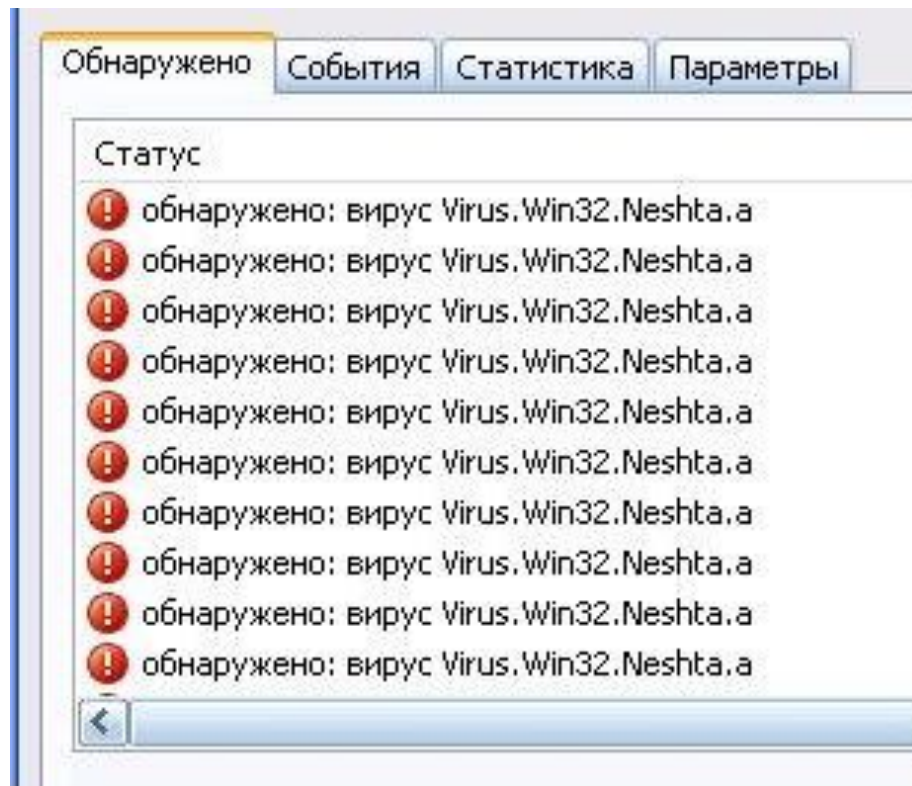


Схема внедрение вируса в начало файла

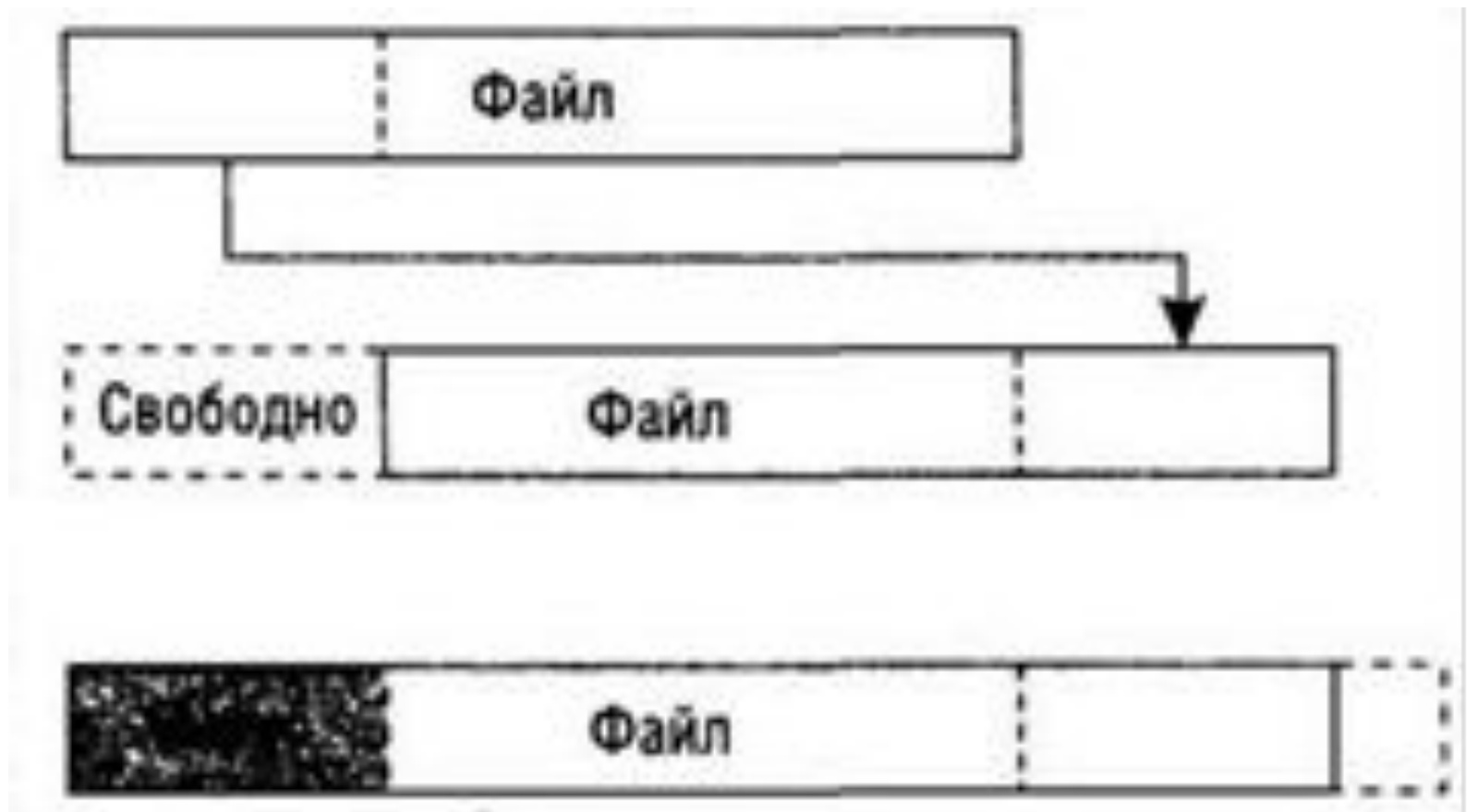


Схема внедрение вируса в файл

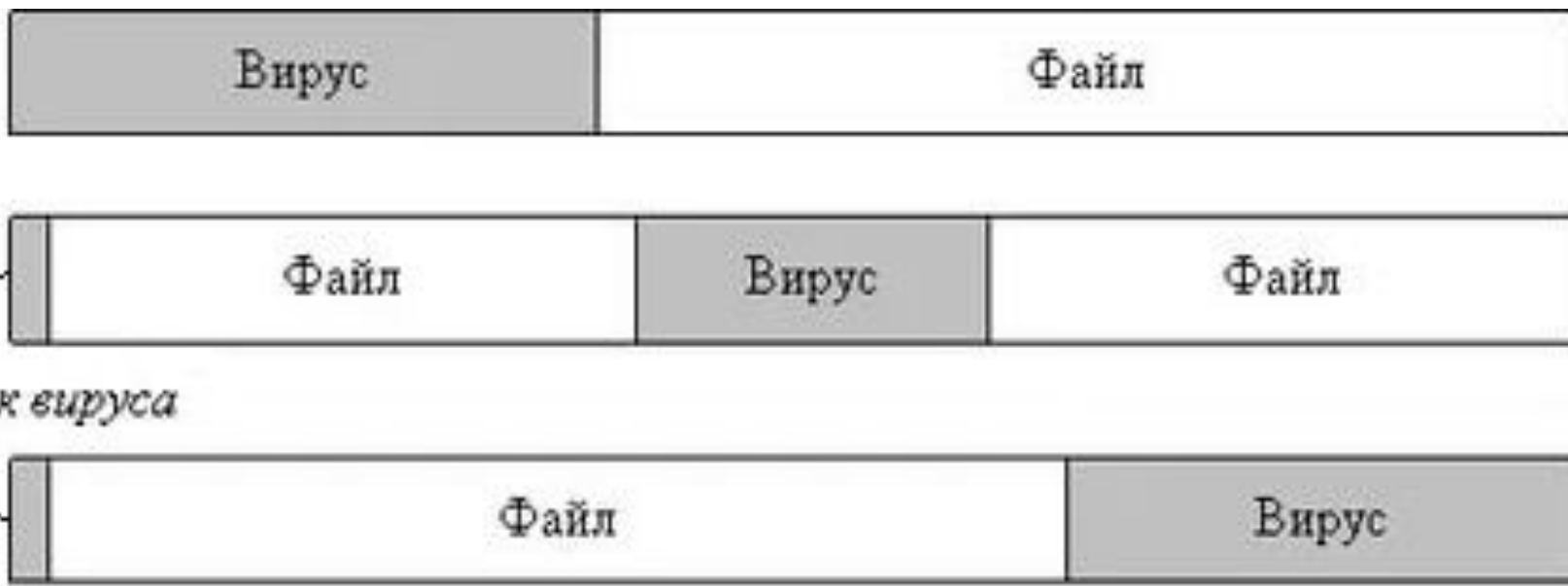


Схема работы вирусов без точки входа



Сообщение об ошибке – вирусная-ссылка.



The site ahead contains malware

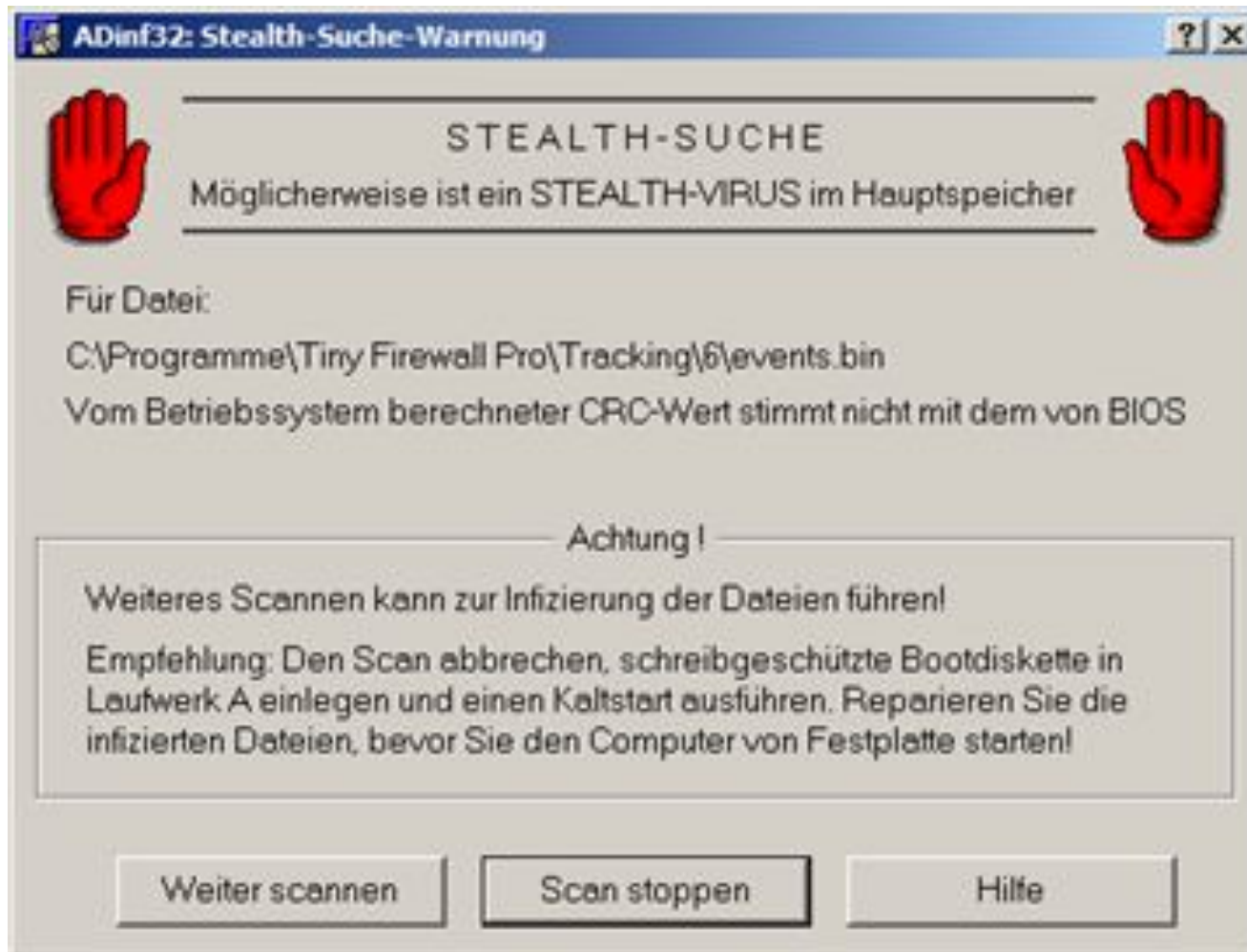
Attackers currently on [soaksoak.ru](#) might attempt to install dangerous programs on your Mac that steal or delete your information (for example, photos, passwords, messages, and credit cards).

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

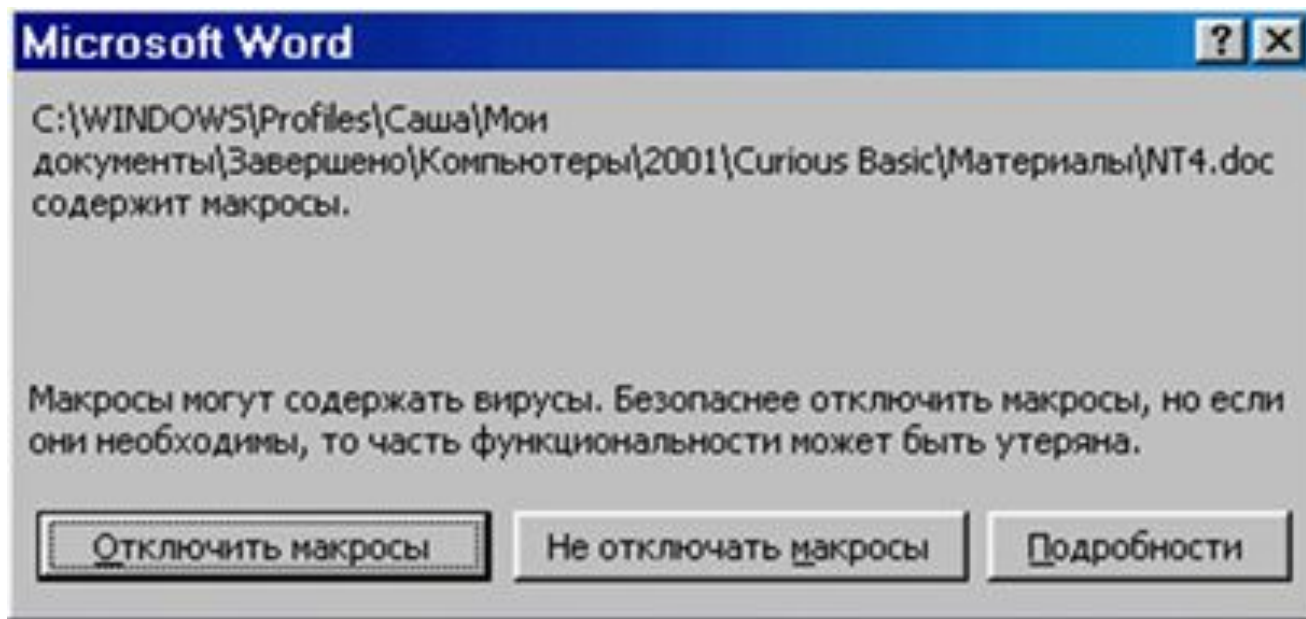
[Details](#)

[Back to safety](#)

Сообщение об ошибке – обнаружение стелс-вируса



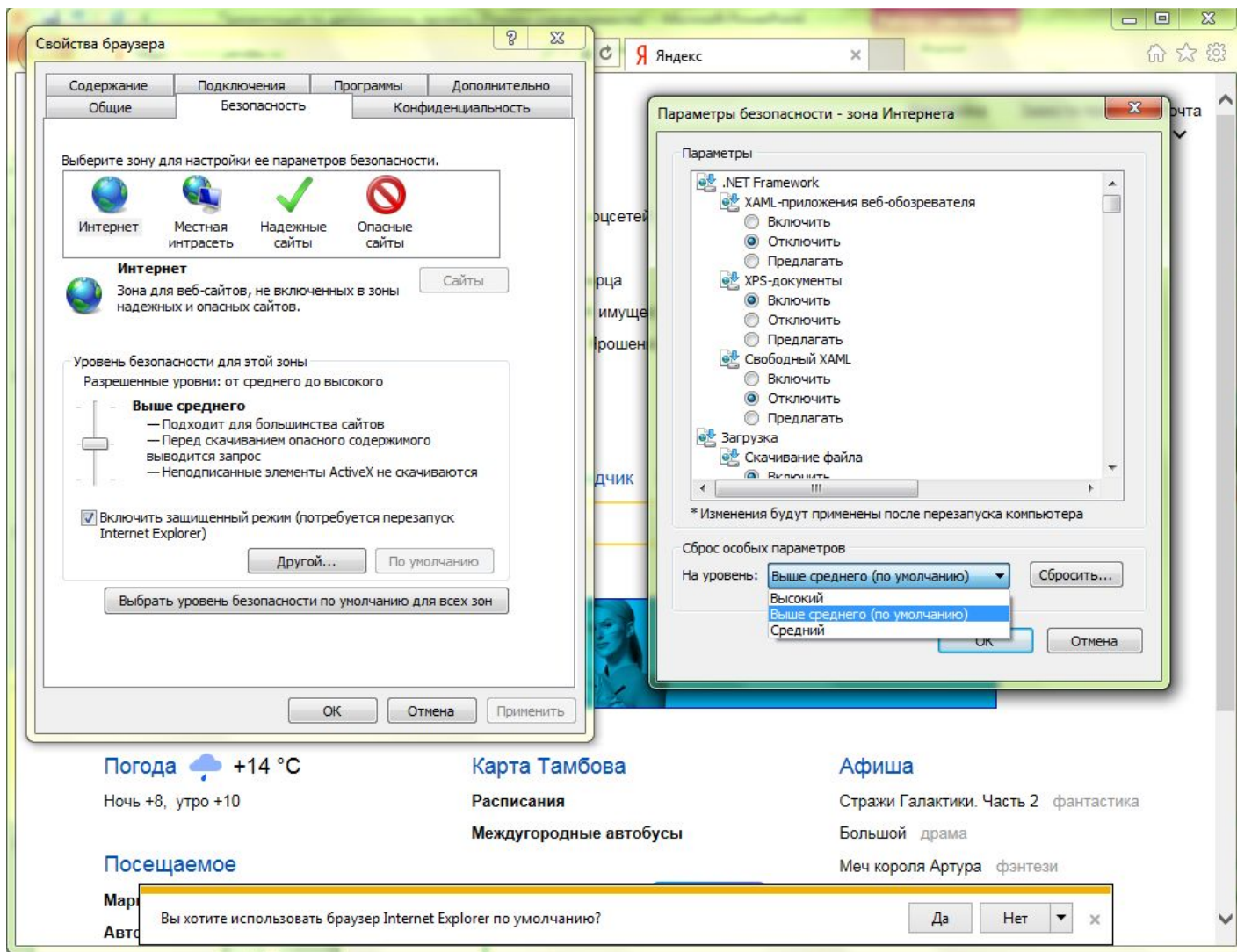
Сообщение об угрозе заражения макровирусом



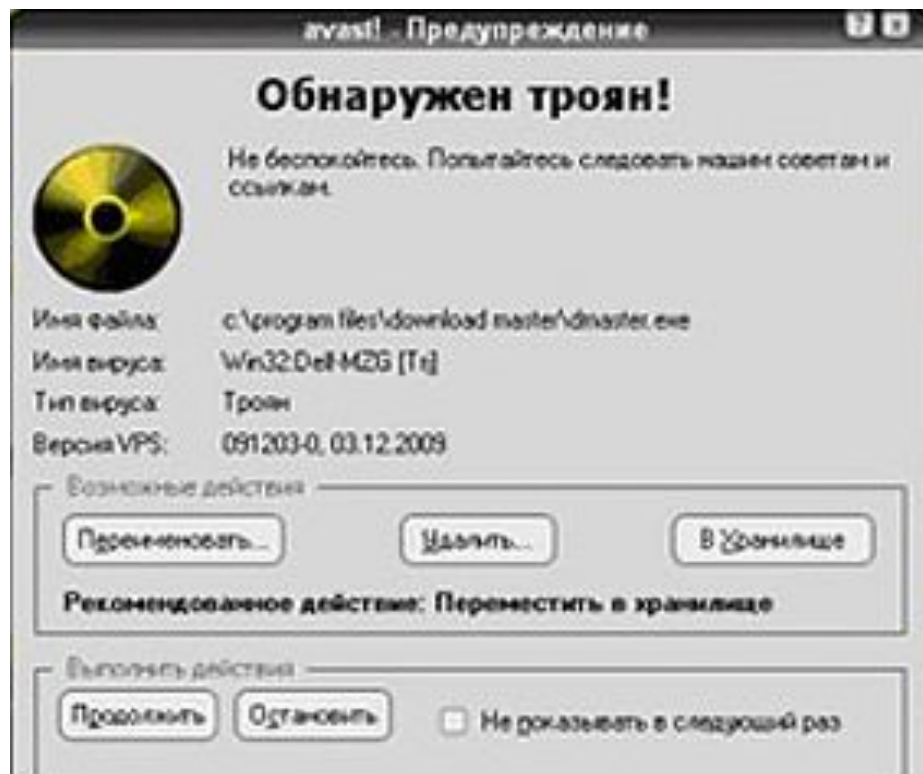
Программный код скрипт-вируса

```
Windows PowerShell
328a35 Reportada como Limpio.
C:\Windows\system32\OLE32\System.Windows.Forms.resources\2.0.0.0_x-ww_4c72a5c561934e889\System.Windows.Forms.resources.dll
11 885ffff77a5aa29582981c958132cdbl Reportada como Limpio.
C:\Program Files\OpenDNS\DNSCrypt\OpenDNSCryptService.exe 6f865de86c7b6ec845f79cc965643626 Reportada como Limpio.
C:\Program Files\OpenDNS\DNSCrypt\dnscrypt-proxy.exe 5188132a0979c88631192795a30a328 No se encuentra en la base de datos de WI.
https://www.virustotal.com/file/289f87266217999c90408f62b59dafaf4c42d81432ebc1d5bab8f3f961764329/analysis/1362913061/
C:\Windows\system32\conhost.exe 318e9119d8a1cfd1da8978078633d81 Reportada como Limpio.
C:\Program Files\NUVIDIA Corporation\NUVIDIA Update Core\dasmenu.exe 81e408bfa53ed15dc784fa34b44b80f Reportada como Limpio.
C:\Windows\system32\cmd.exe ad7b9c14883652bc5321ba57482342b98 Reportada como Limpio.
C:\Windows\system32\MIHRRND.dll 326c7f76a29877a872aa7726e91c1c17 Reportada como Limpio.
C:\Program Files\Foxit Software\Foxit Reader\Foxit Reader.exe 478ccdf7942843c7f24bb4321bb3a13f46 Reportada como Limpio.
C:\Windows\system32\aspfilter.dll 088cf536388f67882f22e4246f812225d Reportada como Limpio.
C:\Windows\system32\SearchProtocolHost.exe e1ac87f5c5252857e4861843e36a6701 Reportada como Limpio.
C:\Windows\system32\MSBooks.dll ac427386c738258f52c86f466a883e8 Reportada como Limpio.
C:\Windows\system32\scaph.dll 4b67c7c82838de812c6485581a7611 Reportada como Limpio.
C:\Windows\system32\MP132.dll 8be9d572c4b2f3be97185bab2afcf5 Reportada como Limpio.
C:\Windows\ms.exe 9b788dc78471a4881d8c9194146f279 Reportada como Limpio.
C:\Windows\System32\Atos.dll 85408d9384726565f1254dc438b43c42 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\Firefox.exe bf21271e12a4b44f4712788f534685 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\mozglue.dll 57ec45fe4243891d68f1d34354f7caf1 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozglue.dll 8a90f549f65524f13e2248714c23f9f Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll a8bc87252226adaffefcd6b5dbec887f Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozCP180.dll 83e7314889f584a14a61c7d3c4862760 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll 8c23d9ab3a688aef71a7c0c55c4fcf77 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\glc4.dll bd79e72cc4d7098e8d4c7613481437c Reportada como Limpio.
C:\Program Files\Mozilla Firefox\glc4.dll e4f52ad5a3a077b3a3ad96c092568a Reportada como Limpio.
C:\Program Files\Mozilla Firefox\winutil.dll 84889147807277474681385bbe7cadda Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs3.dll 4a88796a4b16575e2b3af889722aaab789 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll a79e801fa1376ad558094bbaad6a824 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll 8a802184133543f79c81abb455486c85 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjslite.dll de2af12f6d82f79c25f09f72cd777fc8 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozalloc.dll a7c1f254d94c458ade17e6a727e6649 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\mozjs.dll 83932128e812b53ff588cc8418a481 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\moz.dll 9fa6e0424ca6b6e85c92271482faa1 Reportada como Limpio.
C:\Windows\system32\scodes.dll 7867aa8536f229e7223140977a2897b Reportada como Limpio.
C:\Program Files\Mozilla Firefox\moz.dll 1896f5ec91ba8ab48ccc47174cfff8 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\components\browsercomps.dll 47841291844918761ae1852a53827668 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\moztab3.dll 6189e374cc912745efeddd488c8bba5 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\moztab3.dll ba874c812651488852a9587d78f623d4 Reportada como Limpio.
C:\Program Files\Mozilla Firefox\moztab3.dll d388812a7e8ca6e83f1c2c13339f984 Reportada como Limpio.
C:\Windows\system32\Shell32.dll 2e8c73242258918e8e88b982a5ca5af Reportada como Limpio.
C:\Windows\system32\Shell32\Shell32.dll 8fcd13cd81815d8ff8e1ff439d31118b7 Reportada como Limpio.
C:\Windows\system32\Shell32\parser.dll 15fe887a23b618f18fa4b2d2dc978baf Reportada como Limpio.
C:\Windows\system32\MOZCPU1.dll 126379d58766f2042334418ae1a66df Reportada como Limpio.
C:\Windows\system32\MOZCPU2.dll de6412a79e815a3ba2a27b9cc12537 Reportada como Limpio.
C:\Windows\system32\MOZCPU3.dll 7d34af78a786238cc24edf8cabf87ab Reportada como Limpio.
C:\Windows\system32\MOZCPU4.dll 46a6a92748075a2c38825c4968875a Reportada como Limpio.
C:\Windows\system32\MOZCPU5.dll aba457bf7c7e806e1388371e88f549df Reportada como Limpio.
C:\Program Files\Mozilla Firefox\moztab.dll 84a4884f21711c8384915dc33ec2a7d Reportada como Limpio.
C:\Windows\system32\Facilit.dll a2631c4465380e72876f7716f3924a943 Reportada como Limpio.
C:\Program Files\NUVIDIA Corporation\3D Vision\NV3DVisionStreaming.dll 9548f5c58aa995f33985ba32cd13adaf No se encuentra en la base de datos de WI.
C:\Program Files\NUVIDIA Corporation\3D Vision\NV3DVision.dll 6f84ab8aa812855acha9aalc85ab242 No se encuentra en la base de datos de WI.
C:\Program Files\NUVIDIA Corporation\3D Vision\NV3DPAPI.dll f187564dc311d6c1a1742e5e1858abfe No se encuentra en la base de datos de WI.
C:\Program Files\Classilla\classilla.exe 8888a64967bcbf9ac7021538e5a3c2 Reportada como Limpio.
```

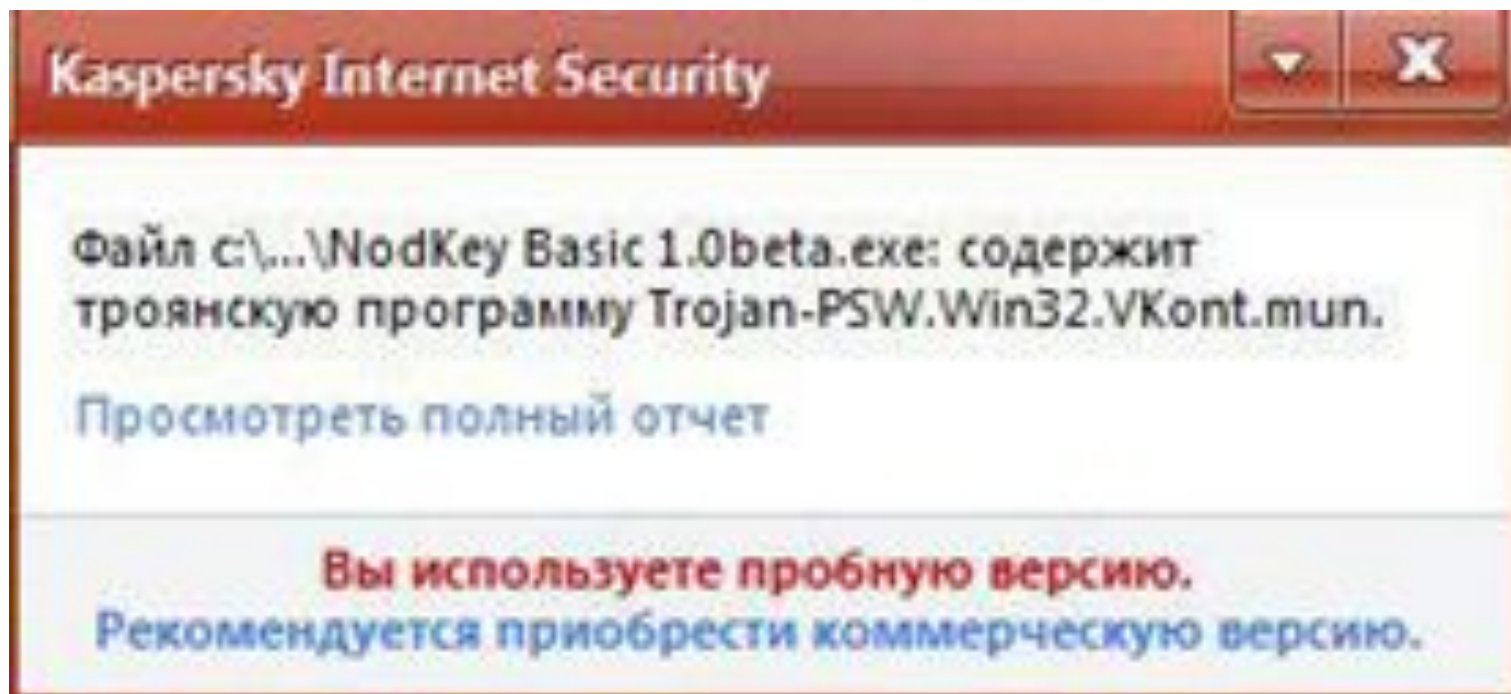

Настройка уровня безопасности Internet Explorer



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.

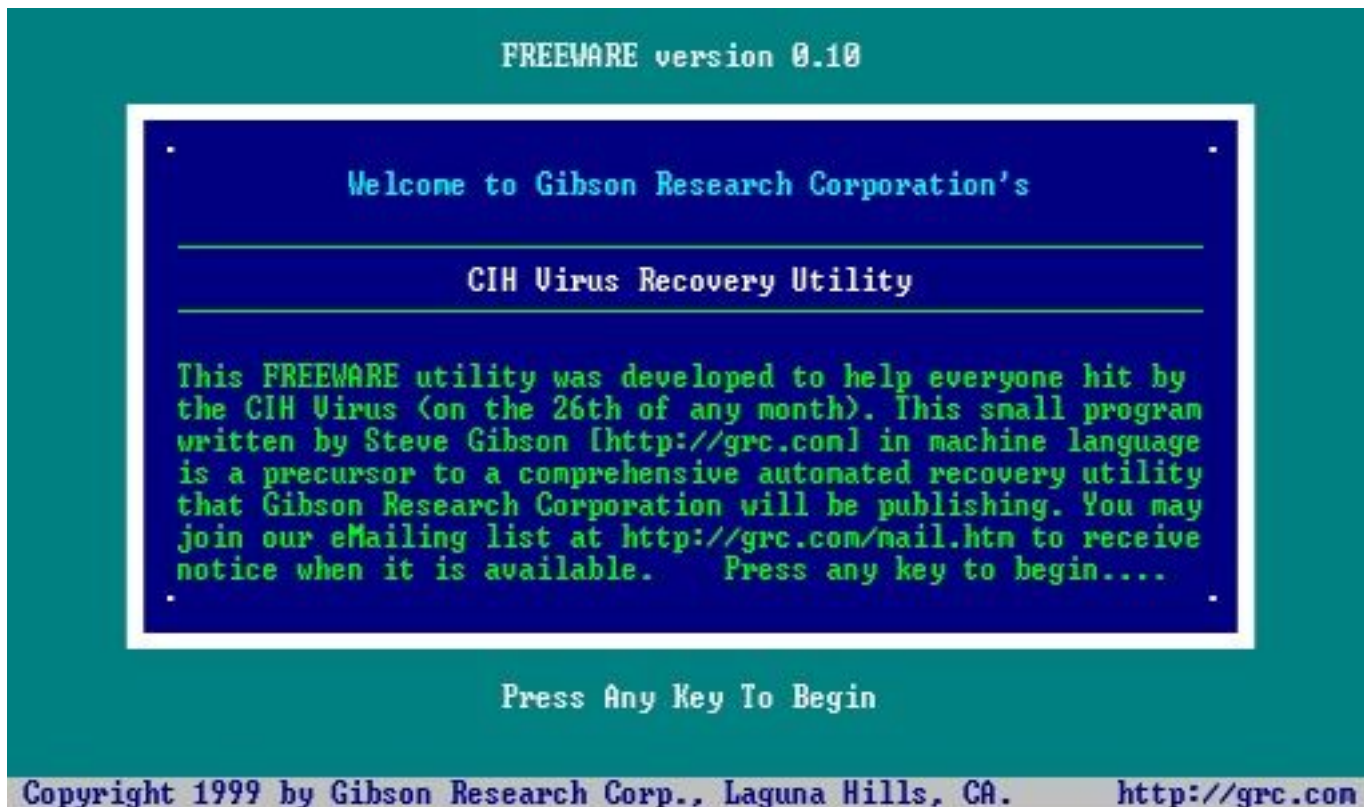
Сетевая атака **not-an-attack:KL-Test-Packet** с адреса 172.16.1.58 была успешно отражена.

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:

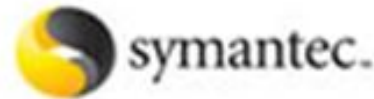
Событие	Время	Путь
локаль... Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38	
на лока... Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38	
на локаль... Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38	
✓ TCP от 225.239.130.214 на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ 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

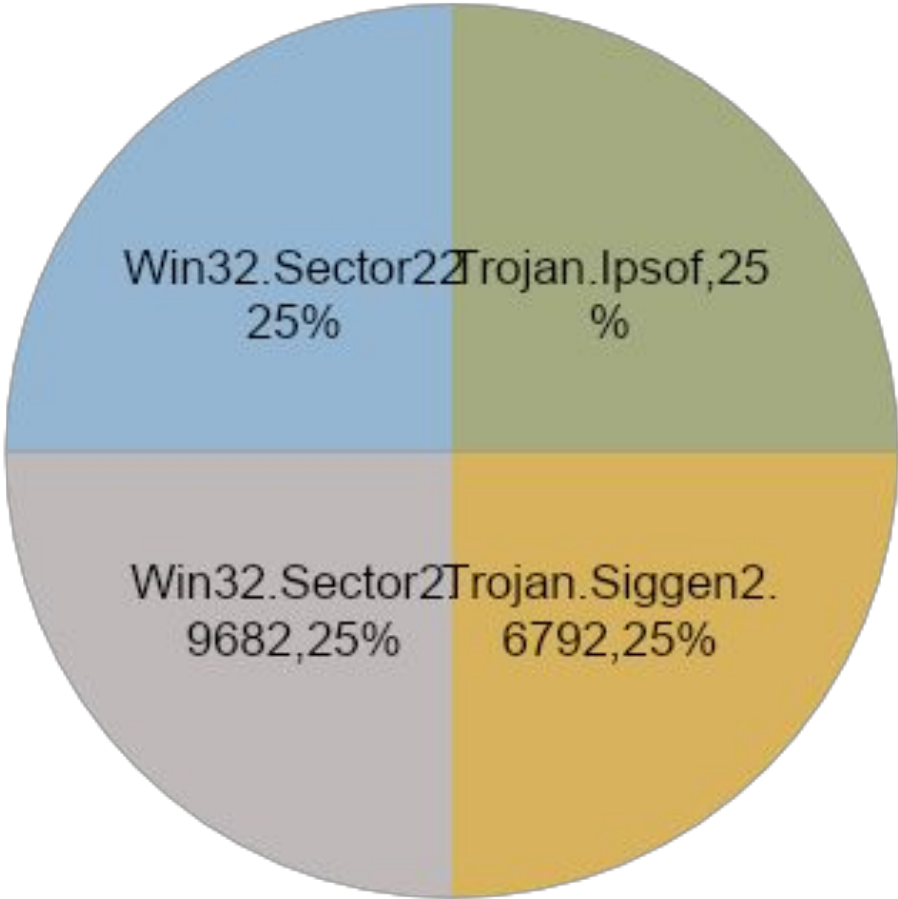


Антивирусные программы принимавшие участие в тесте

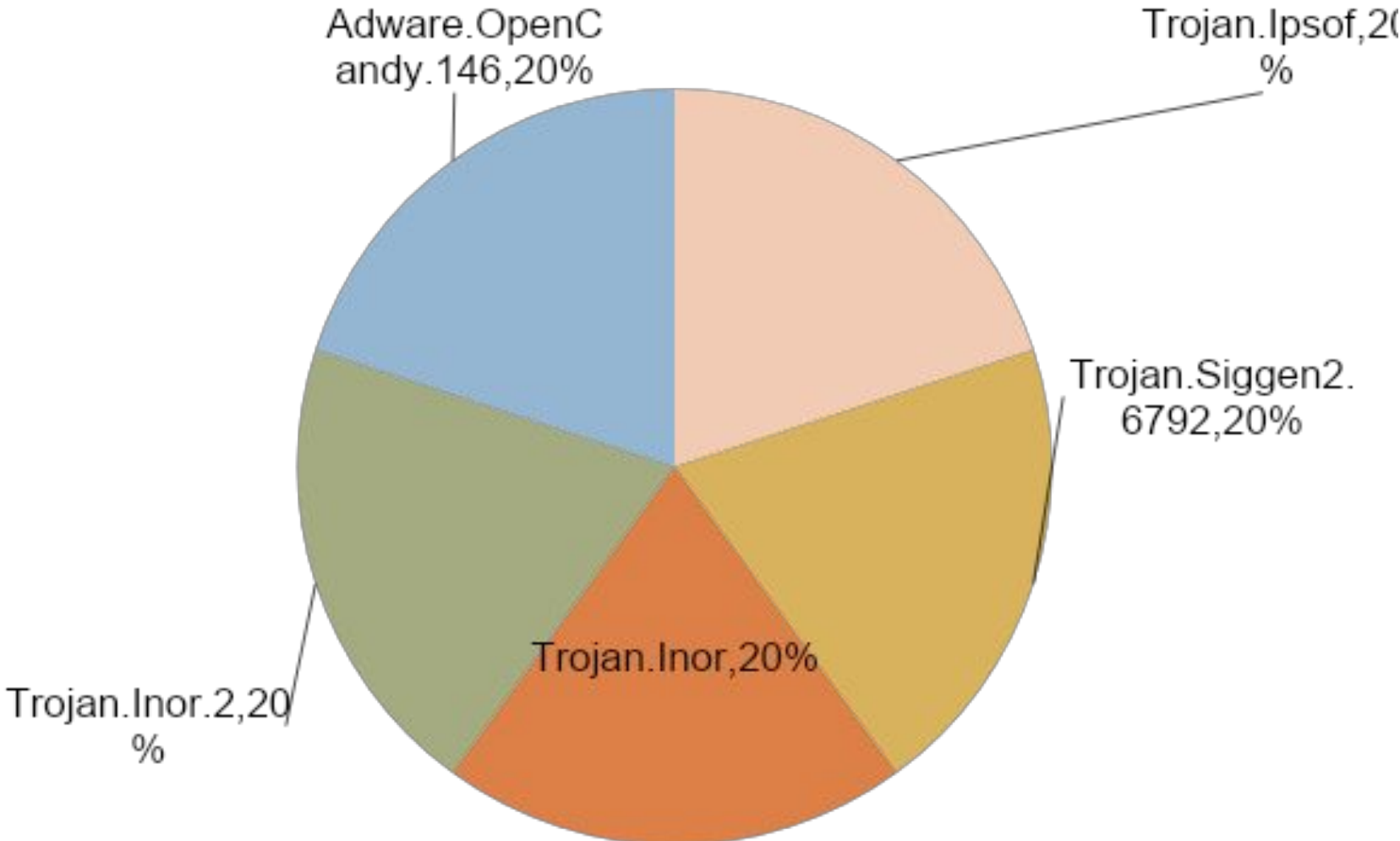
- AVAST Antivirus
- AVG AntiVirus Free
- PC Tools Antivirus
- ESET NOD32 Antivirus
- Norton Antivirus



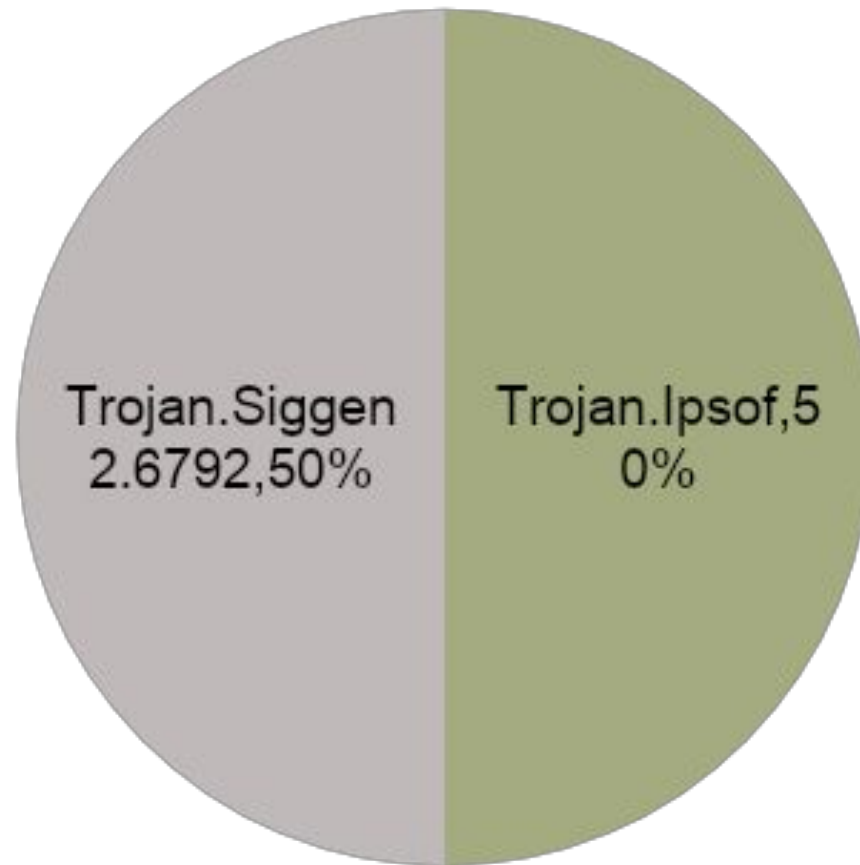
AVAST Antivirus



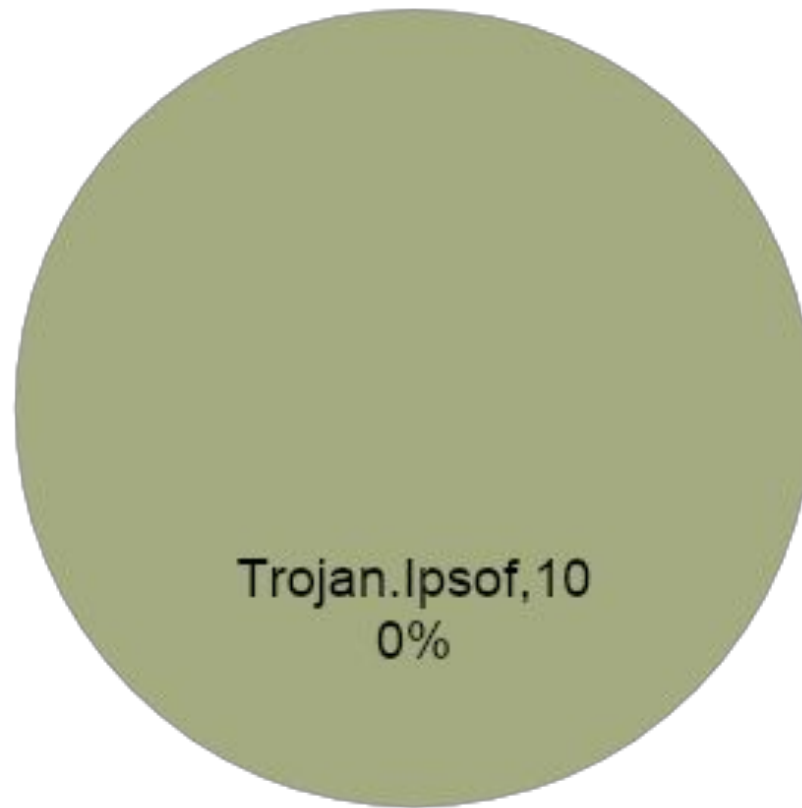
AVG AntiVirus Free



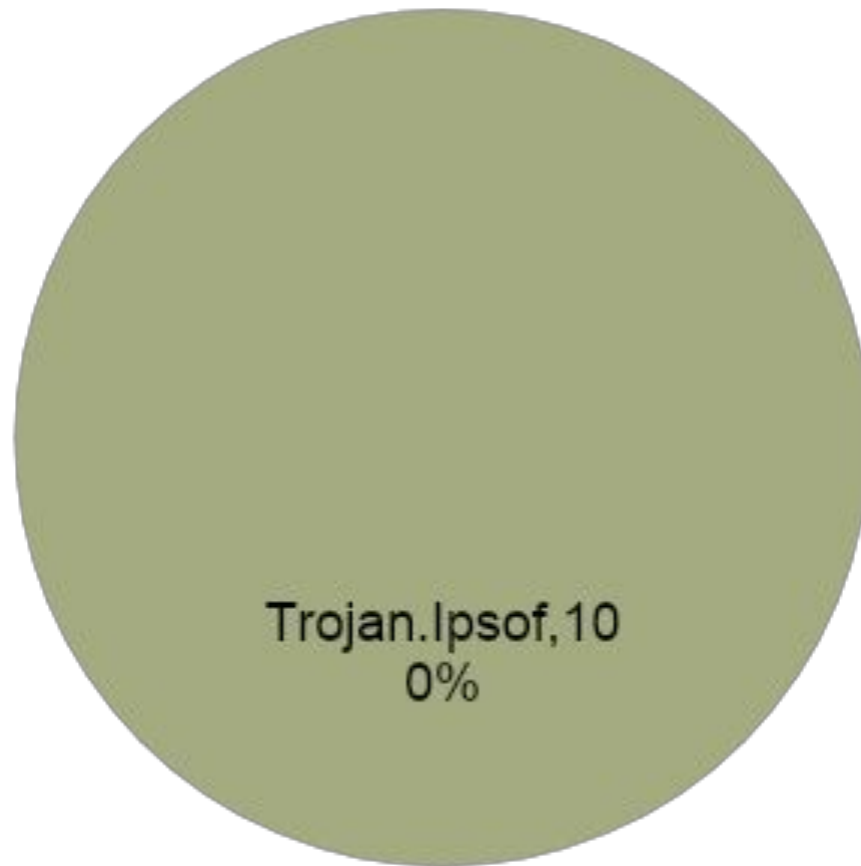
PC Tools Antivirus



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 программы.

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