

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»

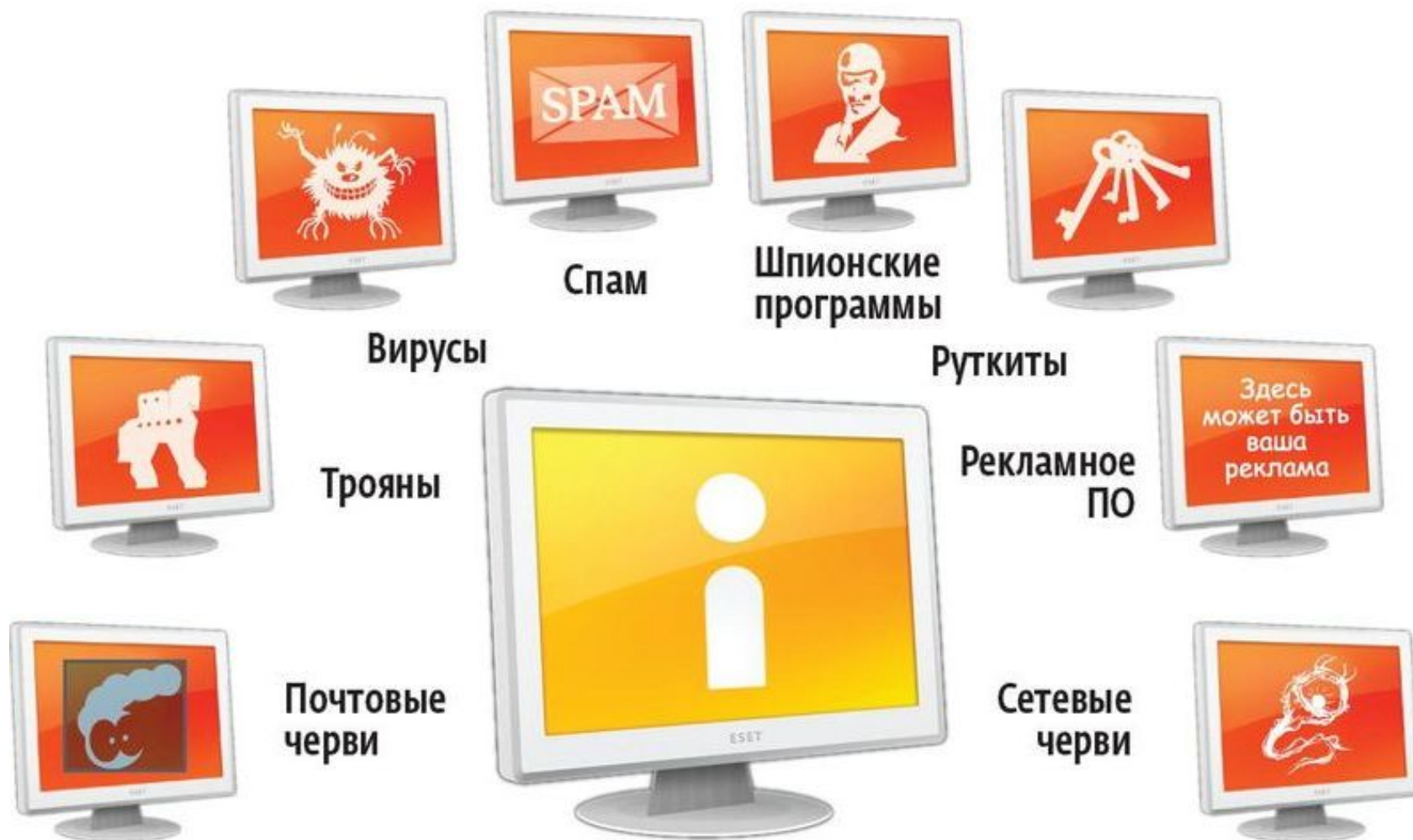
Студента: Ситникова Дмитрия Юрьевича гр. ТАКС – 411

Руководитель проекта: Раздольский В.Е

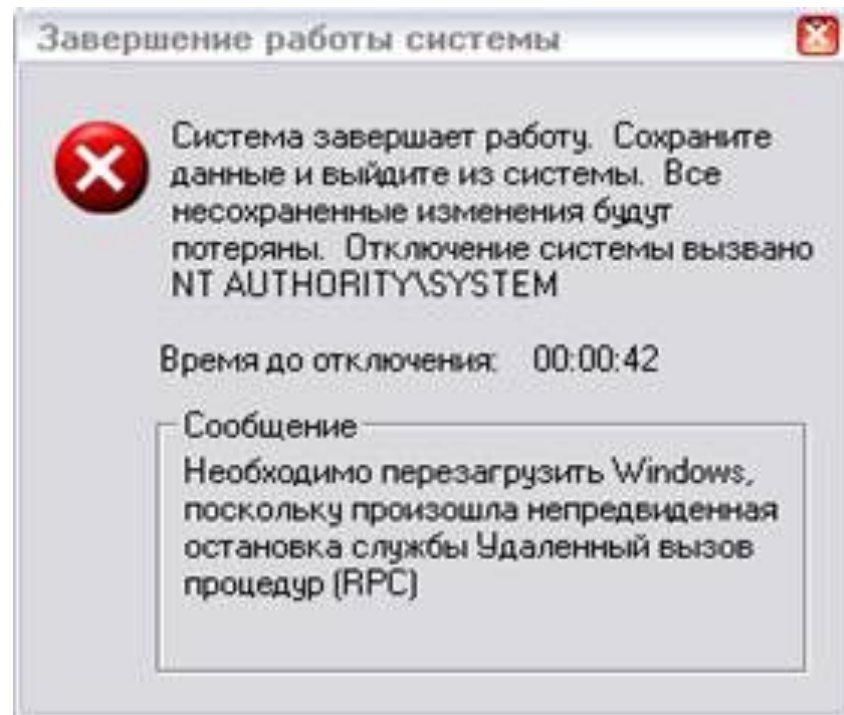
Цели и задачи дипломного проекта

- 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.

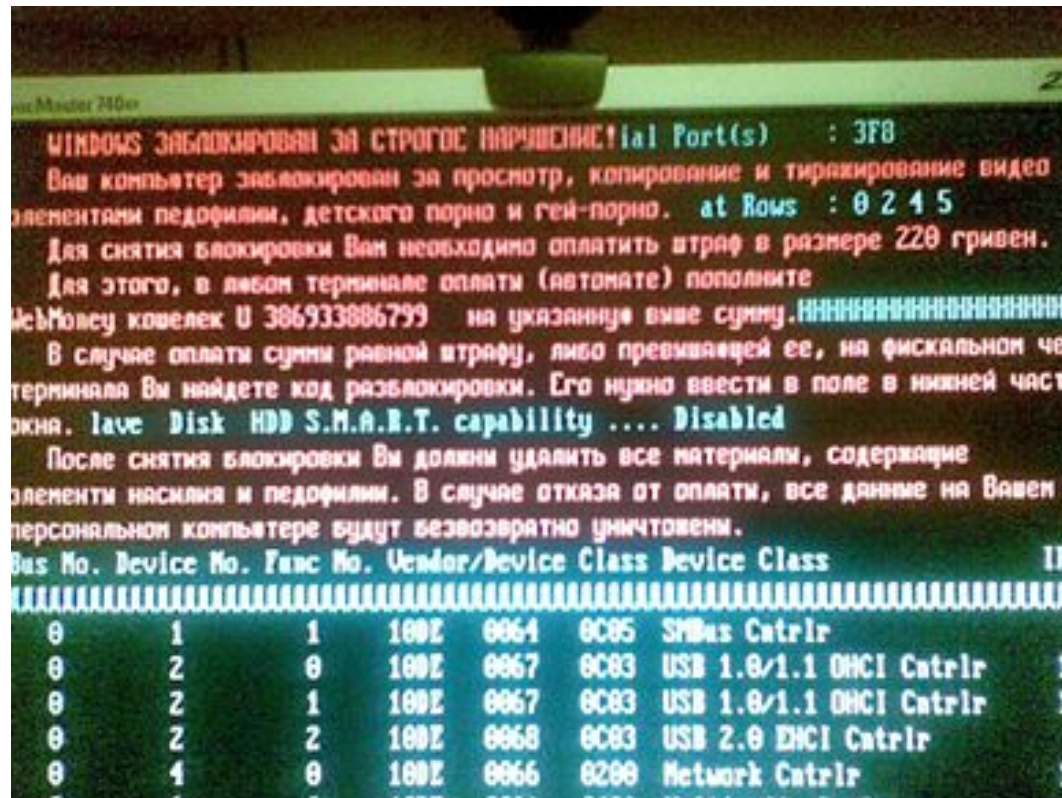
Сетевые угрозы



Сообщение об ошибке – результат работы вируса Blaster



Сообщение об ошибке – Вирус в загрузочном секторе Windows»



Обнаружение файловых вирусов

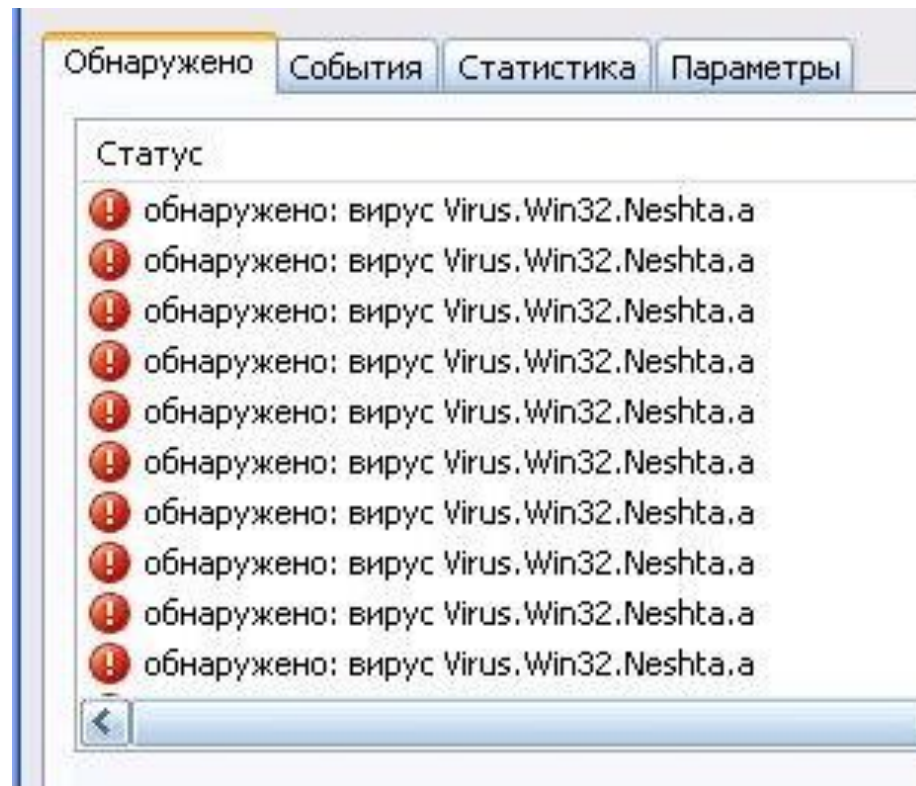


Схема внедрение вируса в начало файла

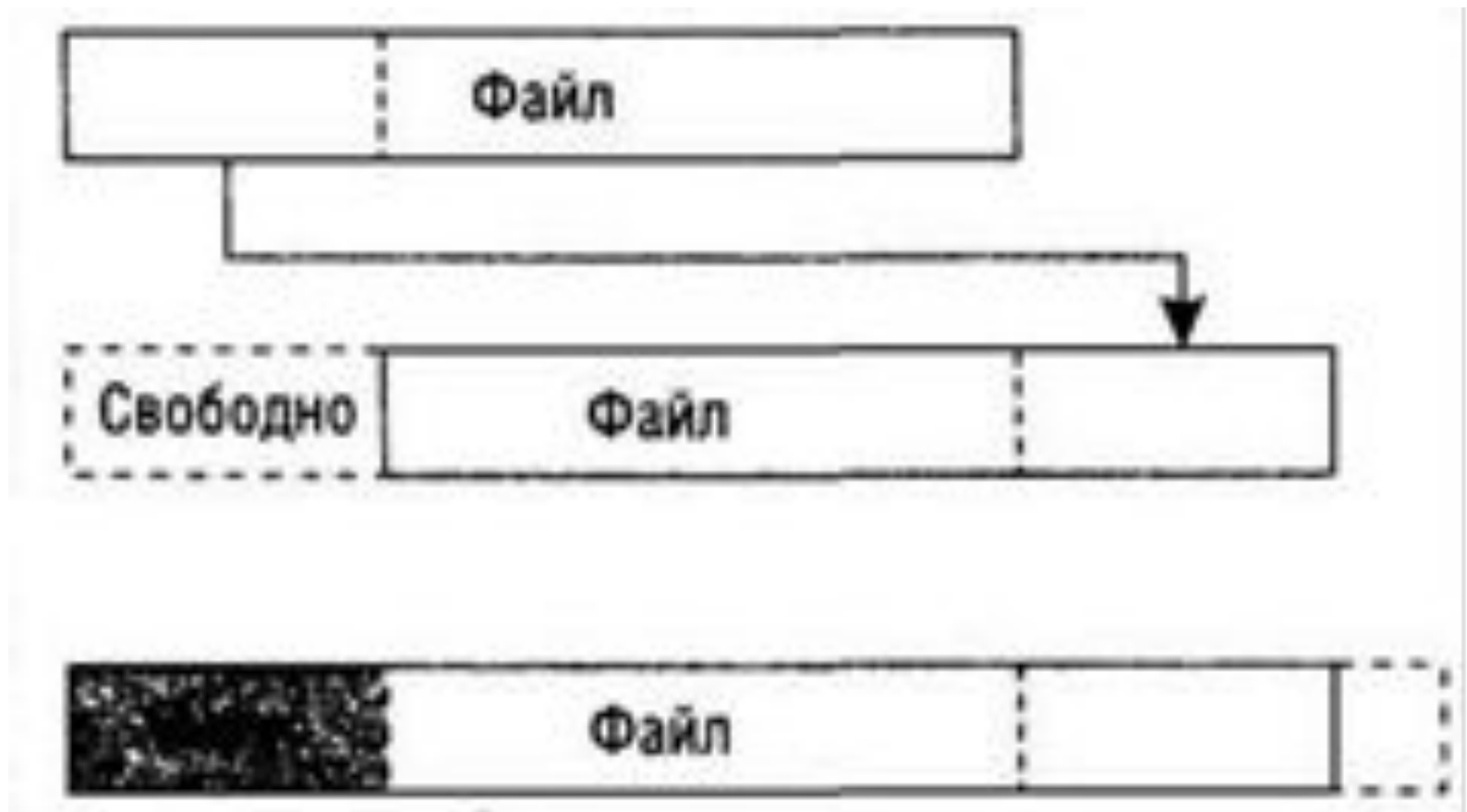


Схема внедрение вируса в файл

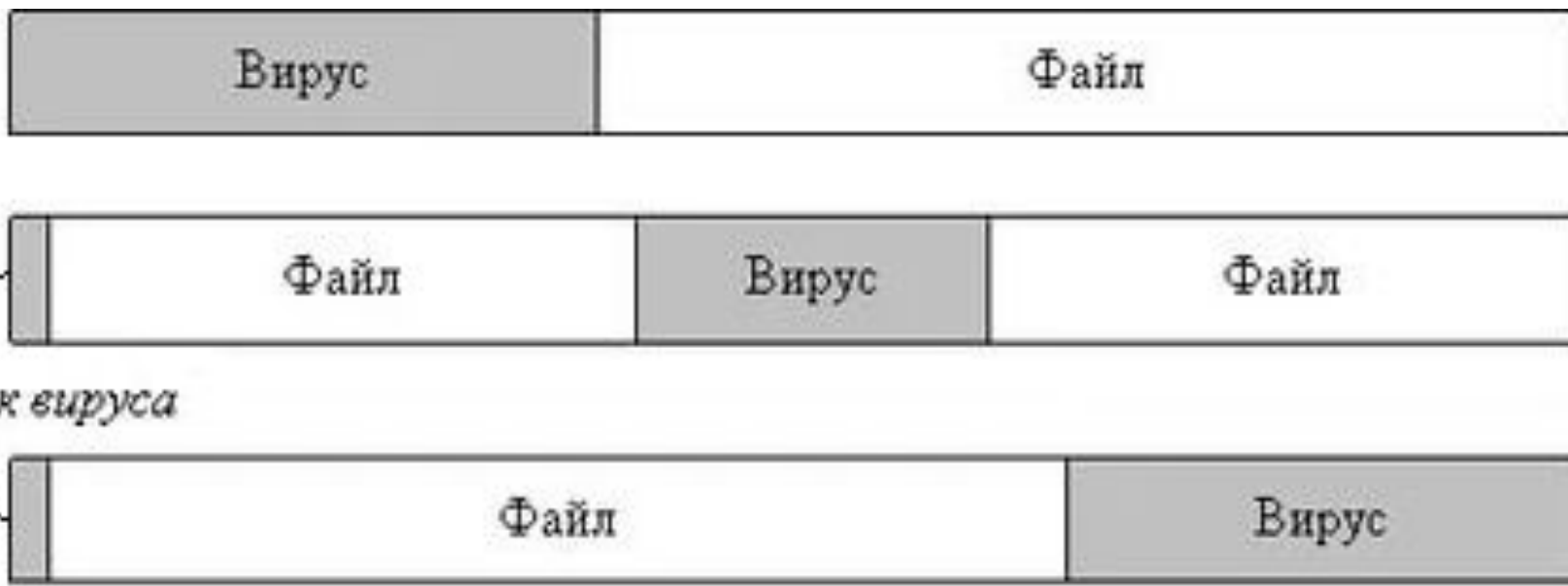


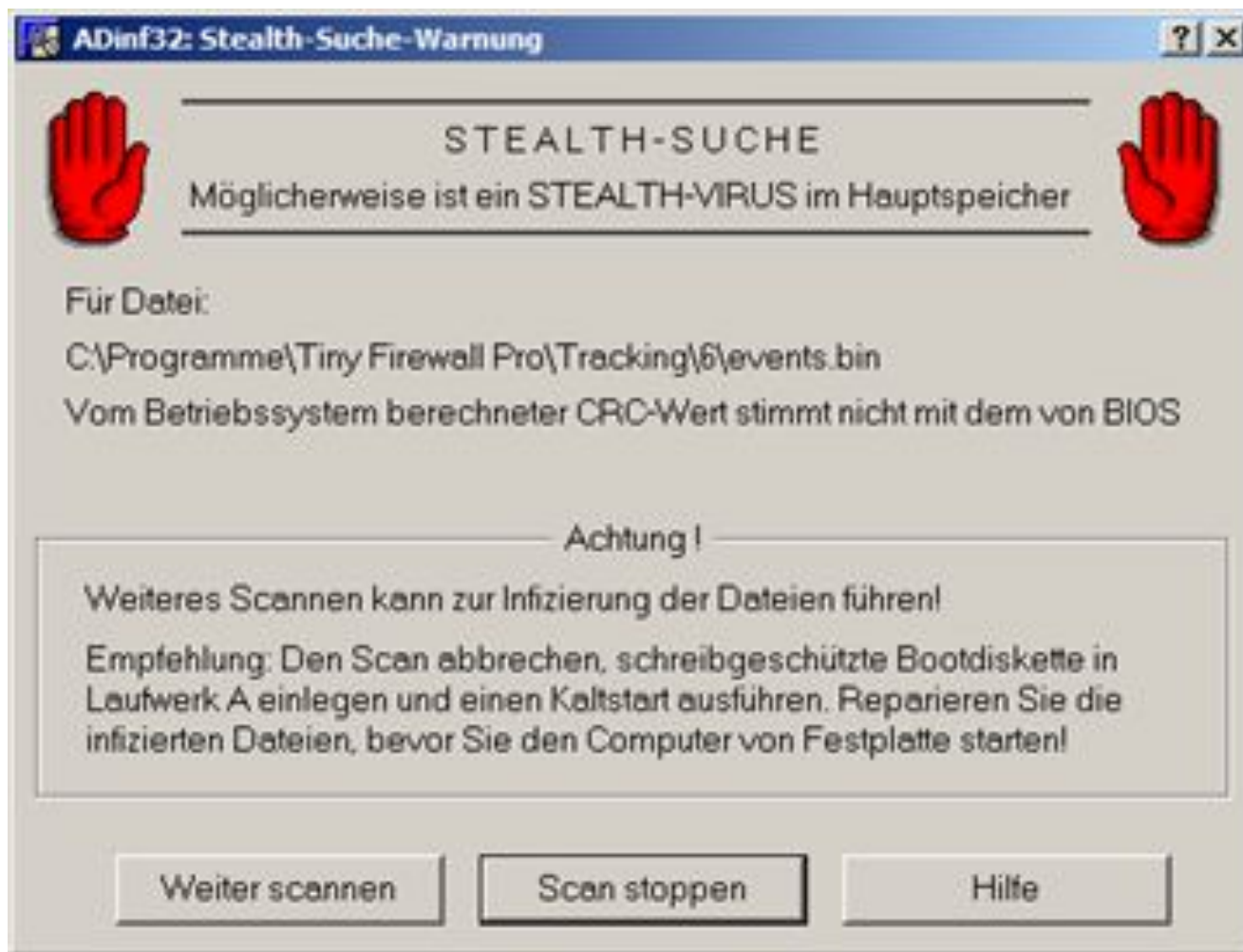
Схема работы вирусов без точки входа



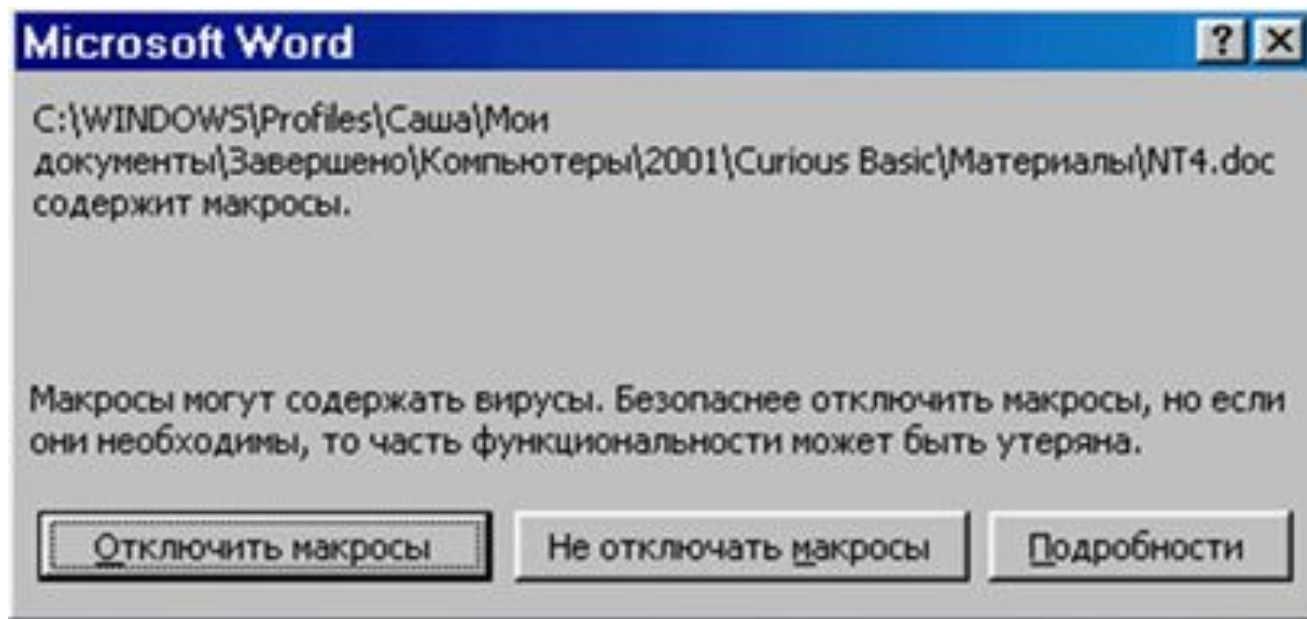
Сообщение об ошибке – вирусная-ссылка.



Сообщение об ошибке – обнаружение стелс-вируса



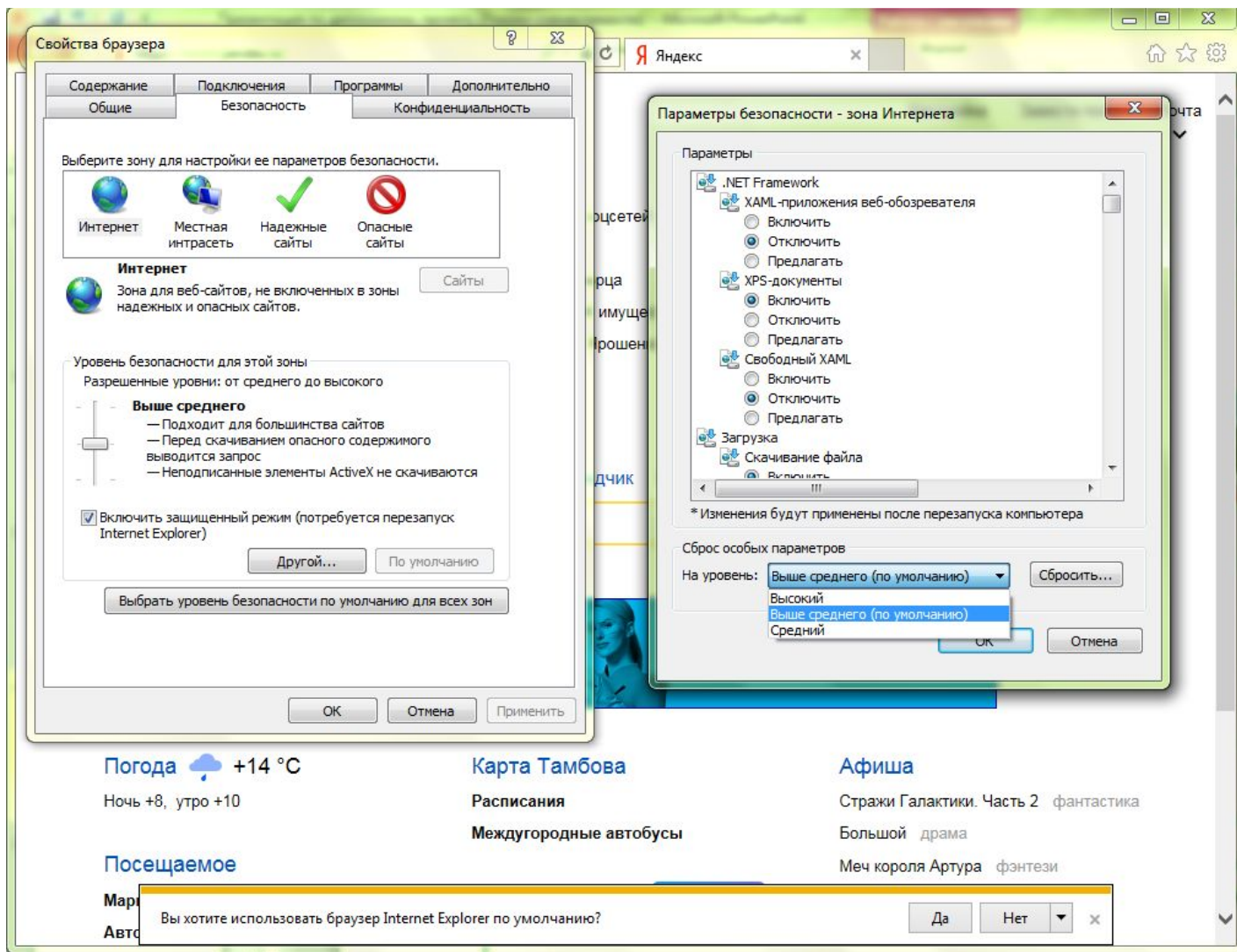
Сообщение об угрозе заражения макровирусом



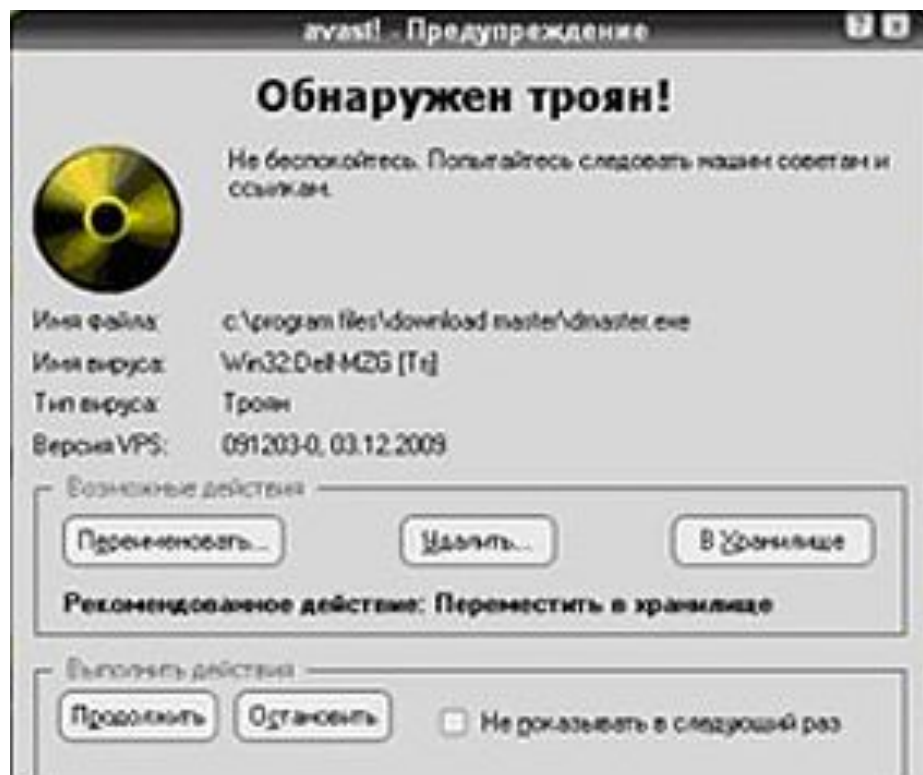
Программный код скрипт-вируса

```
Windows PowerShell
C:\Windows\system32\cmd.exe Reportado como Limpio.
C:\Windows\system32\conhost.exe 318e9119d8a1cf4fda891700796533d81 Reportado como Limpio.
C:\Program Files\OpenDNS\DNSCrypt\OpenDNSCryptService.exe 6f865de86376ec845f79cc765663626 Reportado como Limpio.
C:\Program Files\OpenDNS\DNSCrypt\decrypt_proxy.exe 518d142ca579c86631f92795ab30d180 2a ha encontrado un posible...
https://www.virustotal.com/file/289f872662177979c90408f62b59dafaf4c62d81d32ebc1d5bab0f3f961764329/analysis/1362913061/
C:\Windows\system32\conhost.exe 318e9119d8a1cf4fda891700796533d81 Reportado como Limpio.
C:\Program Files\NVIDIA Corporation\NVIDIA Update Core\danmou.exe 81e10e8bfa53jed15dc784fa34b44bb0f Reportado como L
limpio.
C:\Windows\system32\cmd.exe ad7b9c14883b52ba532fba5748342b98 Reportado como Limpio.
C:\Windows\system32\WINEBND.dll 326c7176a29787a872aa7726e91c1c17 Reportado como Limpio.
C:\Program Files\PeerBlock\peerblock.exe 478ccdf79d2843c9f72bb4321bba13f46 Reportado como Limpio.
C:\Windows\system32\aspcfilt.dll 088cf5b6308f17082f2a4246f812225d Reportado como Limpio.
C:\Windows\system32\SearchProtocolHost.exe e1ac87f6c5252857e4862843c36a6701 Reportado como Limpio.
C:\Windows\system32\MSBooks.dll a6427386473025b052c8a6f4b6a883a8 Reportado como Limpio.
C:\Windows\system32\aspcfilt.dll 4367c7c62818bde812c6486581a7611 Reportado como Limpio.
C:\Windows\system32\MP132.dll 8ba7d872c4b2f3ba89185bca82afcf6 Reportado como Limpio.
C:\Windows\hh.exe 7b70b8c78471a4881d8c91941f6f279 Reportado como Limpio.
C:\Windows\system32\ntcs.dll b540b373a472b565c12544c438b43c42 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox.exe bf2f2717c13a4b44f47f12780534e865 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\NUR180.dll 57ec457e4243801d48f4d34356f7cafa1 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 8a70f549f6552f6f3622248714c33f9f Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe a8bc87252224adaffcf4d6b9d8c80f7f Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 83e7314804f504a14a51c7d3c4b62f60 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe c823d9a3c4d808f71a7c655c4fcff3 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe bd77e72c8cd7078e8d4c7613d81437c Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe a4f52abd3a3a0777b3a3ad76c8d72568a Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 048081d7007277474681385b8e7cadda Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 4a88796a4b16575e2b3af80772aabb709 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe a7be8d1f1376ad5458044bbaad6a5824 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 8a002104133543f794c91abb455d86e85 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe de2af12f6dd82f7c25f00f72cd7777c8 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe a7c1f254d94c458ade17e64727e649 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 83732128b812b53ff508cc8410a601a Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 7fa6e0424c4ab8e85c92271d82faa1 Reportado como Limpio.
C:\Windows\system32\cmd.exe 7069aah8536f29e67223140977a2894b Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 1b965ec91bbaab8d6cc47174c1fba4 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 47641291844018701a1852a53827668 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 6489c374cc912745efedd44b88cb8a5 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe ba874c812651d88552a7587170f636d3 Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe d308812a7e8c6a6e83f1c2c1333f904 Reportado como Limpio.
C:\Windows\system32\Nls\Phone\1.dll 2ech732422509f145e4d808a981a5ca1f Reportado como Limpio.
C:\Windows\system32\Nls\Phone\2.dll 8fcd13c5a818d07f8a1fd37dd111b7 Reportado como Limpio.
C:\Windows\system32\Nls\Phone\3.dll 15f6882a23618f8fa4b2d3d6728baf6 Reportado como Limpio.
C:\Windows\system32\Nls\Phone\4.dll 126b75d58756f2042834418ae1a66df Reportado como Limpio.
C:\Windows\system32\Nls\Phone\5.dll de6412a7ee015a3a3a2a27b7cc12537 Reportado como Limpio.
C:\Windows\system32\Nls\Phone\6.dll 7d34af78a706238cc24edf8cabb87ab Reportado como Limpio.
C:\Windows\system32\Nls\Phone\7.dll 46a8a7274075a2c108f5c496e875a Reportado como Limpio.
C:\Windows\system32\Nls\Phone\8.dll aba457bfc7ec8b6e130837f1e8f549df Reportado como Limpio.
C:\Program Files\Mozilla Firefox\Firefox\Firefox.exe 84a8046f2f711c308d915dc33ec2a7d Reportado como Limpio.
C:\Windows\system32\Facilit.dll a2631c4465b0c72b76771af3924a54d3 Reportado como Limpio.
C:\Program Files\NVIDIA Corporation\3D Vision\Nv3DStreaming.dll 9540f5c58a995f339858a32cd13ad4f No se encuentra en
la base de datos de VT.
C:\Program Files\NVIDIA Corporation\3D Vision\NvStereoApi.dll 6f04ab8a812855a8a9aalc85ab242 No se encuentra en l
a base de datos de VT.
C:\Program Files\NVIDIA Corporation\3D Vision\NvSCPAPI.dll f10756dc311dbcia1742e5e1858abfe No se encuentra en la ba
se de datos de VT.
C:\Program Files\Cisco\Winbox\lanman.exe 0008a66967bcbf9ac7d21538e5a3c2 Reportado como Limpio.
```

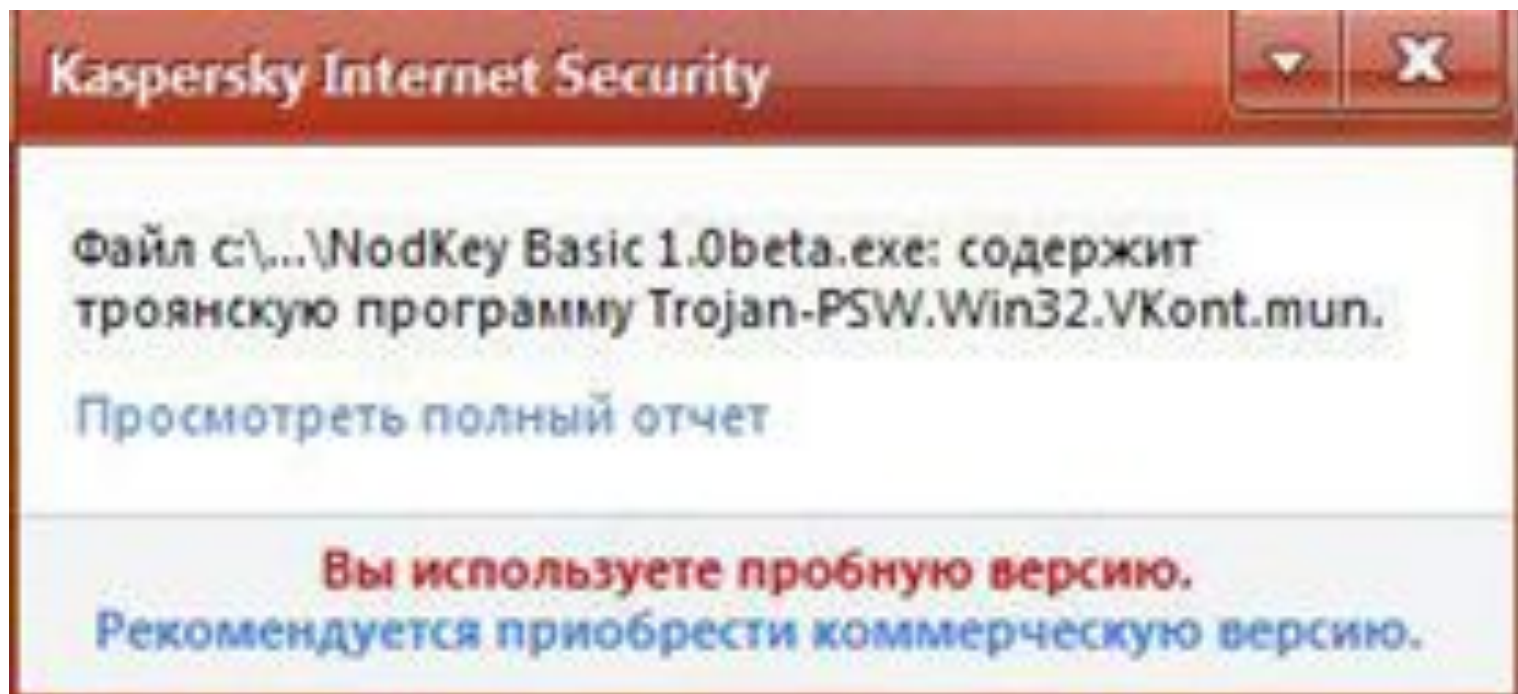

Настройка уровня безопасности Internet Explorer



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.qd](#)

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/#itbsajop=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».



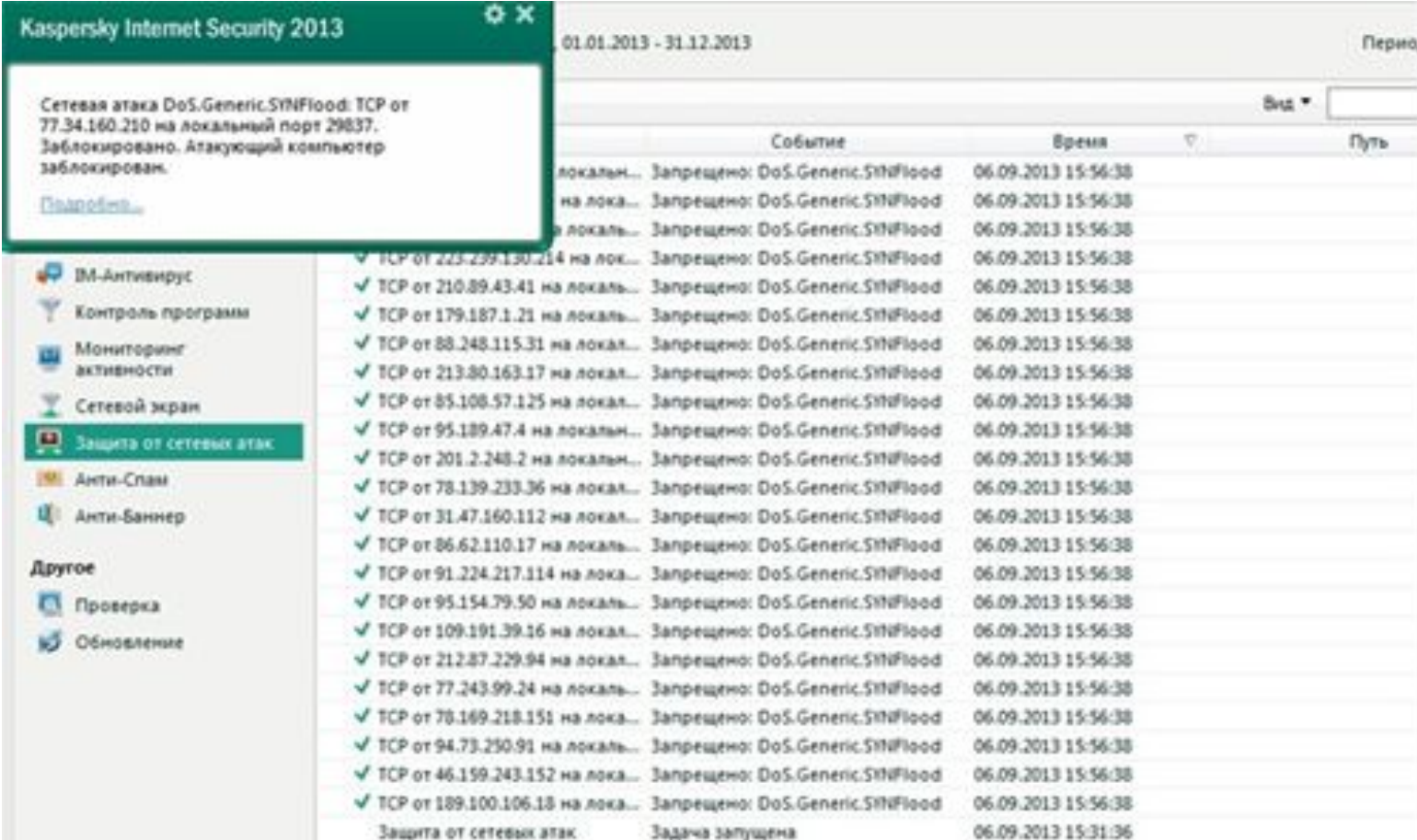
Сообщение об сетевой атаке



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 green notification box in the top-left corner provides details about a network attack: "Сетевая атака DoS.Generic.SYNFlood: TCP от 77.34.160.210 на локальный порт 29837. Заблокировано. Атакующий компьютер заблокирован." Below this, a list of security features is shown on the left, with "Защита от сетевых атак" (Network Attack Protection) highlighted. The main window shows a log of events from 01.01.2013 to 31.12.2013. The log table contains multiple entries of blocked DoS.Generic.SYNFlood attacks.

Касперский Интернет Сьюрити 2013

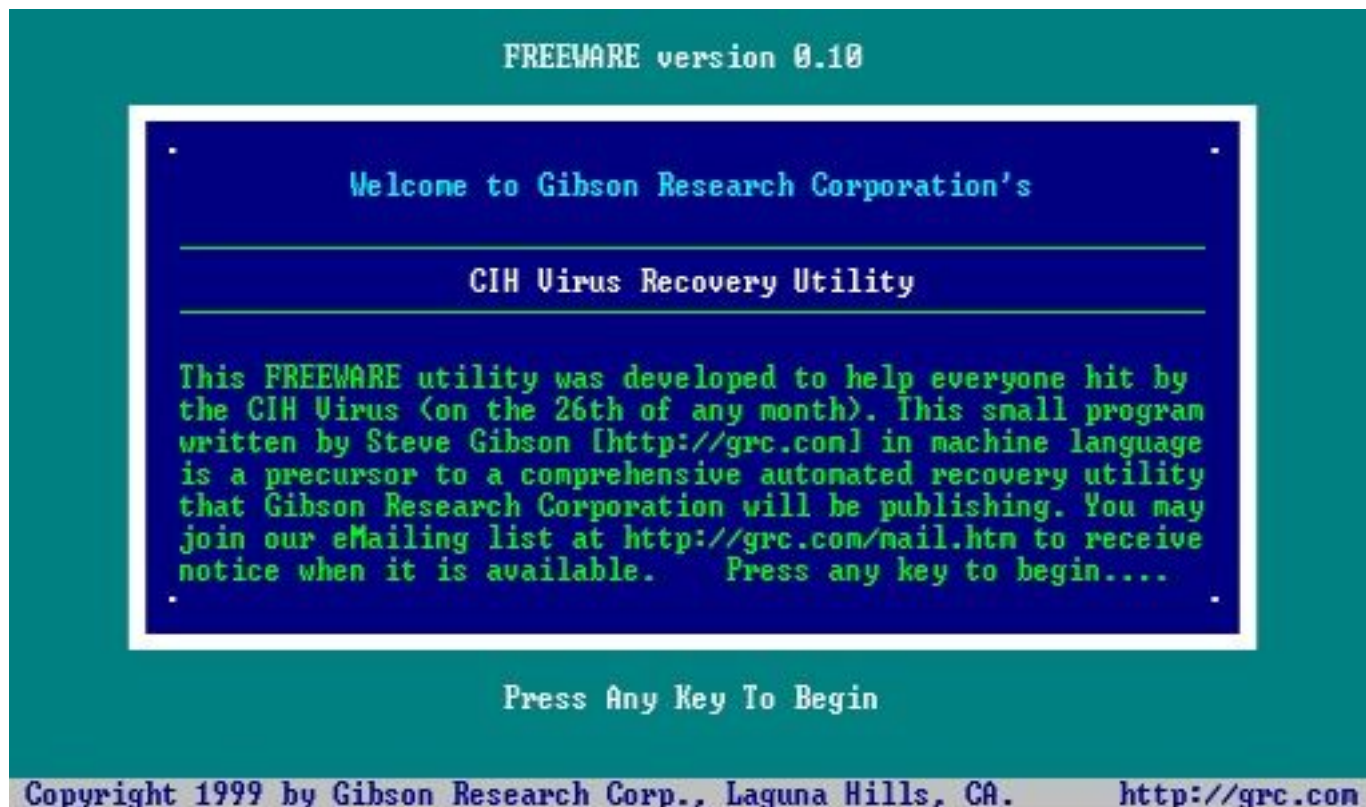
01.01.2013 - 31.12.2013

Сетевая атака DoS.Generic.SYNFlood: TCP от 77.34.160.210 на локальный порт 29837. Заблокировано. Атакующий компьютер заблокирован.

Вид

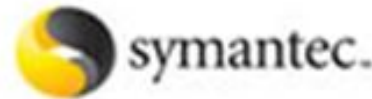
Событие	Время	Путь
локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
а локаль...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP от 223.299.130.214 на лока...	Запрещено: DoS.Generic.SYNFlood	06.09.2013 15:56:38
✓ TCP 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

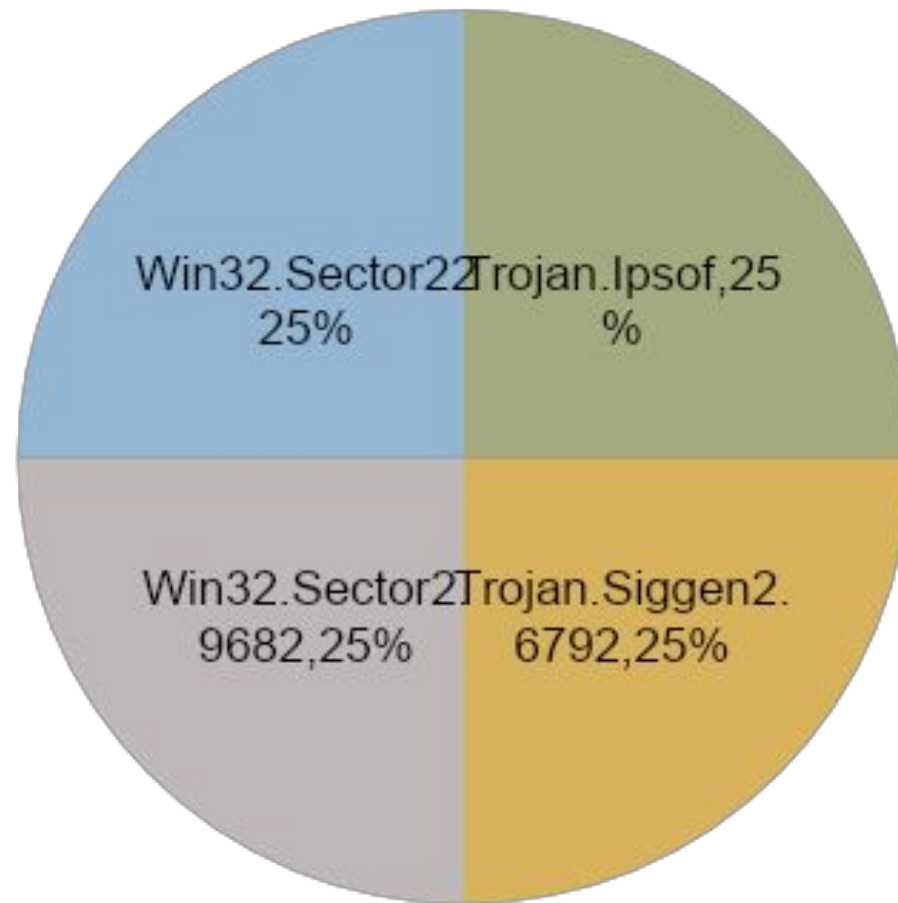


Антивирусные программы принимавшие участие в тесте

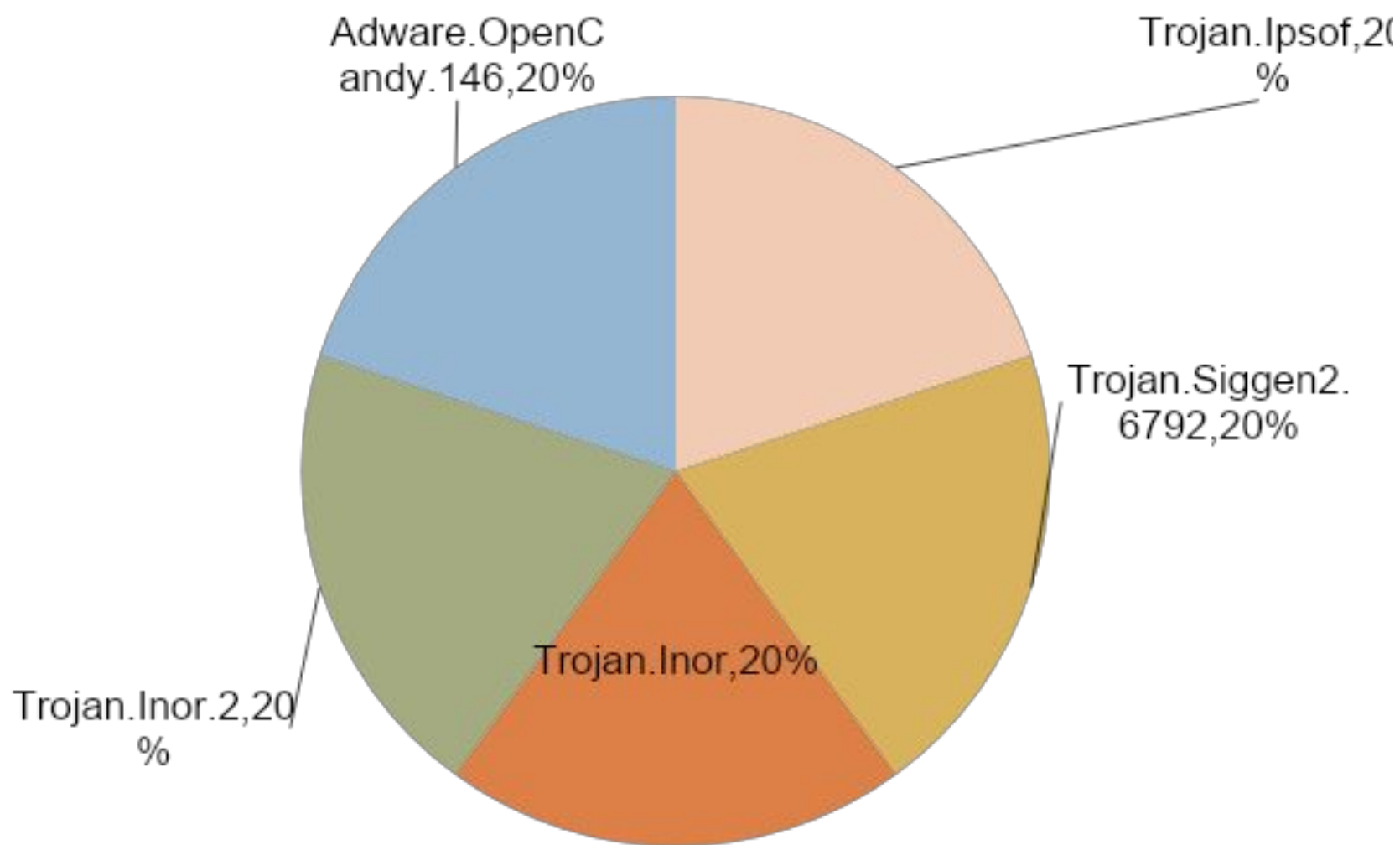
- AVAST Antivirus
- AVG AntiVirus Free
- PC Tools Antivirus
- ESET NOD32 Antivirus
- Norton Antivirus



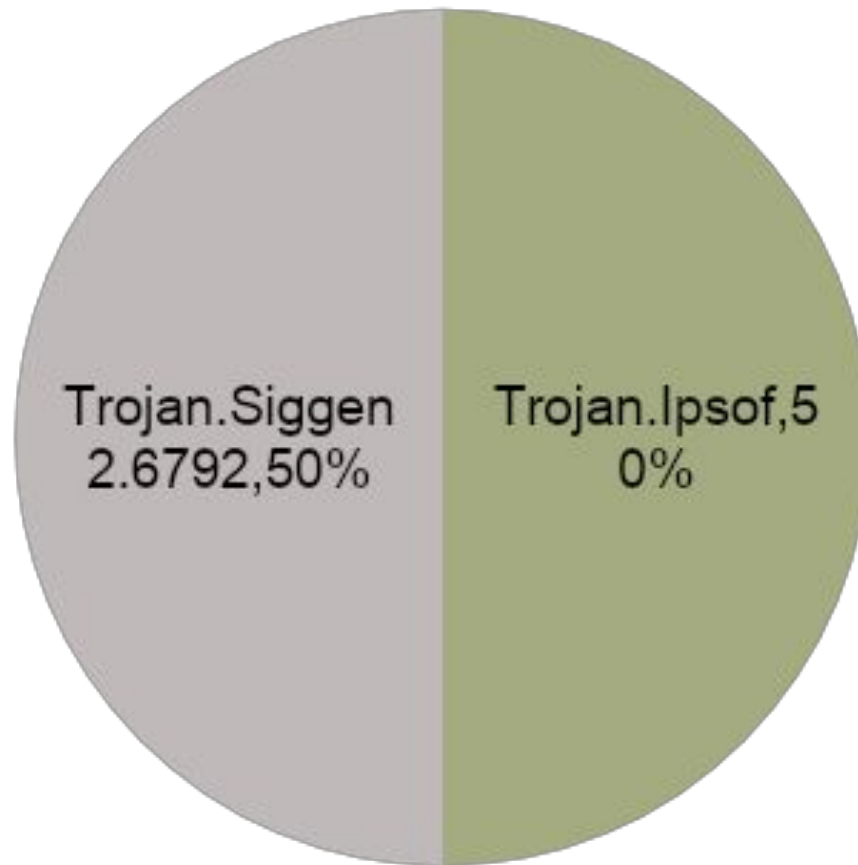
AVAST Antivirus



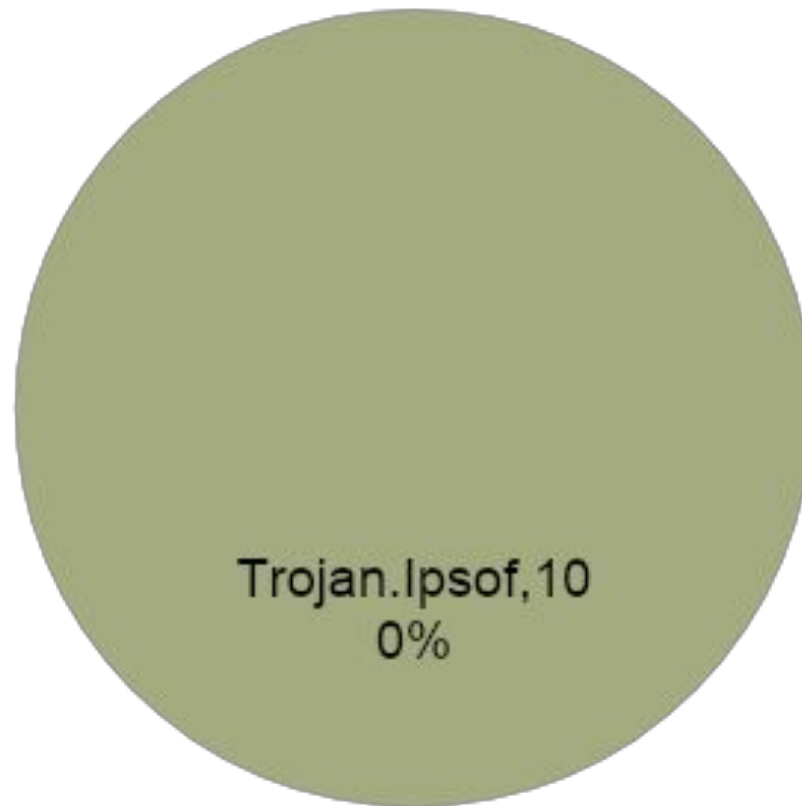
AVG AntiVirus Free



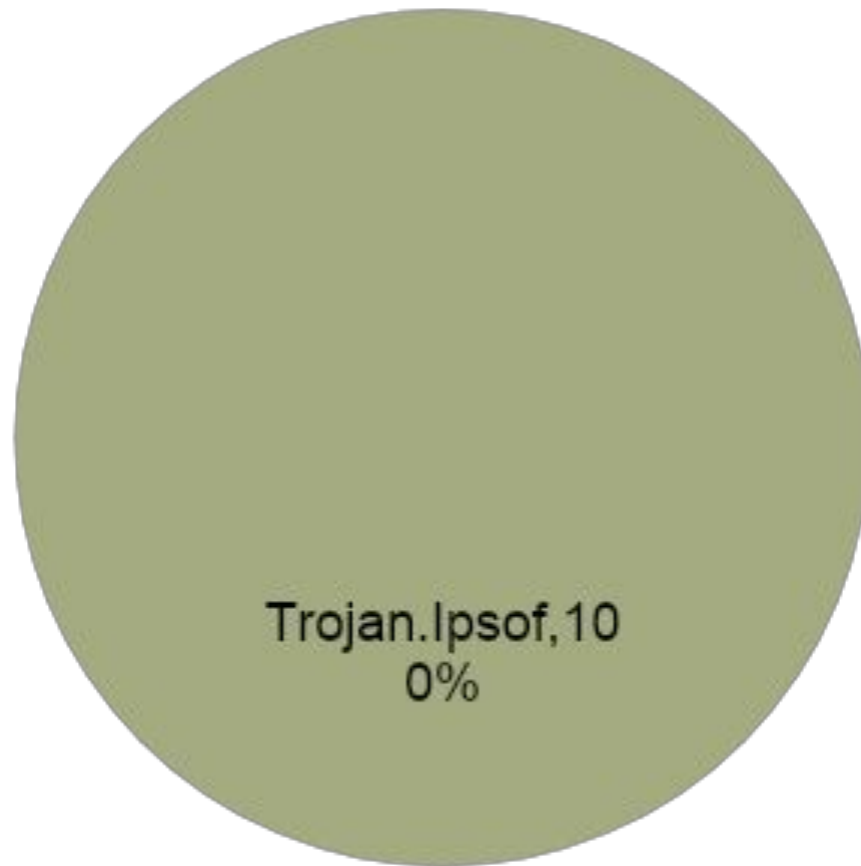
PC Tools Antivirus



ESET NOD32 Antivirus



Norton Antivirus



Dr.Web Enterprise Server



Затраты организации не использующей антивирусное ПО

- ❑ Вирусы выводющие 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