Оглавление

Глава 1

Ashampoo FireWall

Ashampoo Firewall — программа для комплексной защиты компьютера от вирусов и других типов вредоносных программ, а также от хакерских атак и спама. Программа была создана германской частной компанией Ashampoo.

Утилита не является кроссплатформенным программным обеспечением и работает только на компьютерах под управлением операционной системы Microsoft Windows.

1.1. Описание

Мощный и эффективный файерволл, который представляет собой программный комплекс услуг, способный проверять входящие или исходящие данные через Интернет.

После установки в систему Ashampoo Firewall начинает отслеживать всю сетевую активность, контролируя все приложения, исходящий и входящий сетевой трафик, а также защищает компьютер от проникновения хакеров, вирусов, троянских программ, шпионских программ, руткитов, adware по сети или через Интернет. При всех своих больших возможностях остается маленьким по размеру, а также экономным в потреблении системных ресурсов.

1.2. Возможности

- Автоматически определение программы, которая пытается сделать соединения и позволяет пользователю решить, запретить или разрешить действие.
- Два режима защиты.
  - «Easy Mode» — для тех, кто слабо разбирается в тонкостях технической настройки и защите ПК.
  - «Expert Mode» — предназначенный для профессионалов, которые настраивают файрвол под свою ответственность вручную.
- Создание правил для каждой программы.
- Блокирование всего сетевого трафика одним щелчком мыши, в случае обнаружения активного вредоносного кода.
- Минимальное потребление системных ресурсов.
- Компактный и простой в использовании графический интерфейс.
- Подробная статистика о клиентских, серверных, локальных, разрешённых и блокированных соединениях.
- Журнал событий.
- Также в стандартную комплектацию входят 4 дополнительных инструмента для обеспечения безопасности.
  - Интернет очистка (удаление всех следов веб-сёрфинга в сети).
  - Менеджер автозапуска.
  - Блокировщик IP-спама.
  - Мониторинг процессов.

1.3. Примечания

[1] Безопасность: Ashampoo Firewall Free v.1.20. iXBT (12 апреля, 2007). Проверено 9 августа 2010. Архивировано из первоисточника 6 мая 2012.

1.4. Ссылки

- Страница программы Ashampoo Firewall (англ.)
- *Ростислав Панчук.* Обзор бесплатных файрволов. Домашний ПК (29 марта 2007). Проверено 10 августа 2010. Архивировано из первоисточника 6 мая 2012.
- *Юлия Шевченко.* Ashampoo Firewall 1.10: персональная интернет-защита. 3DNews (15 сентября 2006). Проверено 9 августа 2010.

Глава 2

AtGuard

AtGuard — межсетевой экран для персонального компьютера. Основной выполняемой функцией является обеспечение безопасного использования соединения с сетью Интернет. Кроме того, программа может блокировать рекламные баннеры, cookie, JavaScript'ы, элементы ActiveX, а также запретить браузеру передавать конфиденциальную информацию на сервер.

В настоящее время развитие программы как самостоятельного продукта прекращено, он приобретён корпорацией Symantec и встроен в Norton Internet Security.

2.1. Литература

- *FireWall — огненная преграда*//CHIP, июнь 2001
- *AtGuard: на страже*//Компьютерра

Глава 3

Avast!

Avast! — антивирусная программа для операционных систем Windows, Linux, Mac OS, а также для КПК на платформе Palm, Android и Windows CE. Разработка компании AVAST Software, основанной в 1991 году в Чехословакии. Главный офис компании расположен в Праге. Для дома выпускается в виде нескольких версий: платной (Pro Antivirus, Internet Security и Premier) и бесплатной (Free Antivirus) для некоммерческого использования. Также существуют версии для среднего и большого бизнеса (Endpoint Protection, Endpoint Protection Plus, Endpoint Protection Suite и Endpoint Protection Suite Plus) и версии для серверов (File Server Security и Email Server Security). Продукт сертифицирован ICSA Labs.

Название *Avast* является сокращением от anti-virus advanced set («продвинутый антивирусный набор»). То, что в английском языке есть слово avast («стоп»), было замечено позднее.

Avast! Free Antivirus считается самым популярным бесплатным антивирусом. Всего же антивирусом Avast! пользуются более 230 миллионов пользователей во всём мире[1].

3.1. Возможности программы

3.1.1. Основные функции антивируса

- Резидентный антивирусный сканер, работа осуществляется тремя независимыми модулями («экранами»):
  - *Экран файловой системы* — основной компонент сканера в реальном времени. Отслеживает все локальные операции с файлами и папками на компьютере. В его состав входит HIPS, который отслеживает в системе поведение всех программ, действия которых могут напоминать действия вредоносных программ.
  - *Экран почты* — отслеживает весь трафик программ для работы с электронной почтой и сканирует все письма до того, как они попадают на компьютер, таким образом предотвращая возможный вред. Осуществляет проверку трафика по протоколам POP/SMTP/IMAP/NNTP.
  - *Веб-экран* — анализирует все действия пользователя при посещении веб-сайтов в Интернете. Блокирует вредоносные сайты автоматически. Выдает сообщение о блокировке по умолчанию. Начиная с десятой версии контролирует протокол HTTPS.
- Эвристический анализ, эмуляцию программного кода. Эффективен против скрытых в системе руткитов.
- Удаление шпионского программного обеспечения с компьютера.
- Проверка компьютера на вирусы во время показа экранной заставки.
- Проверка компьютера на вирусы во время запуска, до полной загрузки операционной системы. При этом Avast! использует прямой доступ к жёстким дискам, т.е в обход драйверов файловой системы Windows. Avast! — единственный антивирус, в котором встречается подобного рода функция.
- Связь с учётной записью пользователя на официальном сайте Avast!. Появилась с седьмой версии.
- Ряд гибридных технологий для процессов, выполняемых в «Облаке». Включает в себя «Службу репутаций» (для отслеживания репутации определённых файлов и выявления вредоносных) и «Потоковые обновления» (ускоряет обычное обновление антивируса для борьбы с новейшими угрозами). Функция появилась начиная с седьмой версии.
- Компонент DeepScreen позволяет Avast! принимать более обоснованные решения в отношении новых/неизвестных файлов. Является преемником AutoSandbox, начиная с девятой версии. Включает в себя новую технологию: динамическая двоичная трансляция (dynamic binary

translation), а также dyna-gen, представленную ранее. При анализе выдаёт соответствующее сообщение.

- Начиная с шестой версии, бесплатный вариант антивируса включает дополнительную функцию WebRep. Эта функция информирует пользователя о репутации посещаемых сайтов на основании оценок, выставленных сообществом пользователей Avast!. Работает в браузерах Internet Explorer, Mozilla Firefox и Google Chrome. В седьмой версии реализована и для Opera. В девятой версии переименована в Avast! Online Security.
- Начиная с восьмой версии в антивирус входит функция Software Updater, которая позволяет отслеживать устаревшие версии программ и своевременно их обновлять. В версии Avast! Premier программы можно обновлять полностью в автоматическом режиме. Если необходимо обновить программы, которые могут поставить под угрозу безопасность системы, Avast! выдаёт сообщение.
- Дистанционная помощь другим пользователям антивируса, позволяет устанавливать соединение и демонстрировать друг другу рабочие столы компьютеров. Для этого один пользователь генерирует в окне антивируса специальный код, который потом высылается тому, с кем необходимо установить связь. Появилась с седьмой версии.
- Служба «Очистка браузера» удаляет нежелательные расширения браузеров, и контролирует их в Internet Explorer. Также появилась с восьмой версии. Её можно скачать, как автономную программу, если на компьютере нет установленного Avast!.
- Avast! Rescue Disc позволяет пользователям создавать аварийный загрузочный диск или флэш-носитель с антивирусом Avast! на нём. Появился в девятой версии.
- Проверка домашней сети на наличие уязвимостей. Появилась с десятой версии.
- «Интеллектуальное сканирование», объединяющее по запросу все другие виды сканирования (проверку на вирусы, безопасность домашней сети и т. д.). Появилась с десятой версии.
- Блокировка определённых веб-сайтов по их адресу. Может использоваться в качестве родительского контроля. Появилась с шестой версии, а в девятой объединена с Веб-экраном.
- Усиленный режим для более строгих сценариев блокировки. Рекомендуется специально для начинающих пользователей: он автоматически блокирует выполнение бинарных файлов, которые обычно глубоко внедряются в систему (средний уровень), или разрешает выполнение программ только с хорошим рейтингом в FileRep (агрессивный уровень). Появился в девятой версии.
- Автоматическое обновление антивирусных баз, а также самой программы. Сюда же относится и возможность автоматического обновления до более совершенной версии продукта, если был введён лицензионный ключ.
- Настройка плиток, позволяющих пользователю выводить в главном окне антивируса самые необходимые ему функции. Возможность появилась в девятой версии.
- Голосовые сообщения при обнаружении вредоносной программы, успешном обновлении вирусной базы данных и завершении сканирования. Одновременно с этим в нижнем правом углу экрана появляется соответствующее сообщение. До пятой версии использовался мужской голос. Начиная с пятой — женский. Также на официальном сайте можно найти и другие голоса на разных языках (на русском языке дополнительных голосов пока нет).
- Игровой режим, в котором сообщения антивируса не отображаются.
- Возможность установки пароля на изменение настроек программы.
- Возможность делать резервные копии настроек. Появилась с седьмой версии.
- Функция формирования ежемесячного отчёта по безопасности. Можно также выполнить и вручную. Появилась с шестой версии.
- Многоязычный интерфейс, поддержка 44 языков.
- Полностью локализованное справочное руководство.

3.1.2. Функции из платных версий антивируса

- Встроенный брандмауэр. Контролирует все приложения, отправляющие и принимающие данные из Интернета. Отсутствует в версии *Pro Antivirus*.
- Встроенный антиспам. Применяется для фильтрации нежелательных писем рекламного содержания. Также отсутствует в версии *Pro Antivirus*.

- *Sandbox* — песочница по требованию. В отличие от *AutoSandbox*, пользователь может сам выбрать, какие приложения запустить в песочнице.
- Технология *SafeZone* (изолированного рабочего стола). Антивирус создаёт изолированный рабочий стол с встроенным браузером *Avast! SafeZone Browser*, созданным на основе Chromium. Предназначен для абсолютно анонимной работы в Интернете и проведения банковских операций.
- Функция *AccessAnyware*, позволяющая управлять данными на удалённом компьютере. Присутствует в версии *Premier*.
- Безвозвратное уничтожение данных (*Data Shredder*). Присутствует в версии Premier.
- Антивирусный сканер командной строки. Начиная с седьмой версии есть в версии *Pro Antivirus*.
- Полная блокировка сети по требованию (переключение в автономный режим).
- Служба *SecureLine* на основе виртуальной частной сети (VPN), которая защищает и делает анонимными соединения через открытые сети WiFi. На данную услугу нужен отдельный ключ лицензии, активировать который возможно и в бесплатном варианте антивируса. Может устанавливаться отдельно. Появилась с восьмой версии.
- *Avast! Cleanup* (до 13 июля 2015 года назывался *GrimeFighter*) удаляет мусорные файлы и оптимизирует систему. Может устанавливаться отдельно. Появилась с девятой версии.

3.1.3. Функции из бизнес-ориентированных и серверных версий антивируса

- Комплексная защита конечных точек для настольных компьютеров и ноутбуков.
- Сканирование трафика, обрабатываемого серверами.
- Тесная интеграция с серверами SharePoint посредством собственных AV-интерфейсов Microsoft.
- Защита почтовых серверов. Поддержка неограниченного количества почтовых ящиков, при условии, что каждый ящик имеет лицензию.
- Централизованное удалённое управление — способность сетевых администраторов управлять установками и обновлениями всех компьютеров в сети при помощи единой централизованной консоли.

3.1.4. Не актуальные

- Ведение VRDB (Virus Recover Database) — базы восстановления испорченных исполняемых файлов. Использовалось до пятой версии.
- Поддержка скинов (тем оформления), начиная с пятой версии эта возможность отсутствует.
- До девятой версии резидентный антивирусный сканер включал следующие экраны:
  - *Экран P2P* — отслеживал загрузки большинства клиентов файлообменных сетей и торрент-клиентов.
  - *Экран интернет-чатов* — перехватывал все загрузки из приложений для мгновенного обмена сообщениями и проверял их на отсутствие вирусов.
  - *Сетевой экран* — встроенный в программу облегчённый межсетевой экран (IDS, Intrusion Detection System — система обнаружения вторжений). Отслеживал всю сетевую активность и блокировал вирусы, пытающиеся заразить систему через сеть. Кроме того, экран блокировал доступ к известным вредоносным веб-сайтам.
  - *Экран сценариев* — перехватывал все сценарии, выполняемые в системе, как локальные, так и удалённые. До шестой версии эта возможность присутствовала только в платных версиях, затем стала доступна и пользователям бесплатной версии. Начиная с девятой версии объединён с Веб-экраном.
  - Экран поведения - отслеживал в системе руткиты низкого уровня; поведение, напоминающее действие вредоносных программ; неразрешенные изменения. Заменен на HIPS.
- Автоматическая песочница (AutoSandbox). Позволяла запускать подозрительные приложения в изолированной от остальной системы среде, но только для тех приложений, которые по мнению Avast! считались подозрительными. Окно приложения, находящегося в песочнице, выделялось красной рамочкой. В случае обнаружения у программы вредоносных свойств, она закрывалась без сохранения результатов её работы. В бесплатной версии появилась, начиная с шестой версии. AutoSandbox являлась частью Экрана файловой системы. Начиная с девятой версии заменена компонентом DeepScreen.
- В седьмой версии можно было выбрать обычную установку или установку в режиме совместимости в качестве второго антивируса.

- Также в седьмой версии присутствовал модуль SiteCorrect, предназначенный для контроля правильности вводимых адресов сайтов.

- В восьмой версии для Internet Explorer можно было установить блокировщик рекламы.

3.2. Различия между версиями программы

Антивирус Avast! выпускается в следующих версиях[2][3]:

3.2.1. Версии для домашнего использования

- **Avast! Free Antivirus** (ранее *Home Edition*) — бесплатная версия антивируса для домашнего (не коммерческого) использования. Считается самым популярным бесплатным антивирусом в мире. Содержит все основные функции, необходимые домашнему пользователю. С момента установки работает 30 дней, затем требует бесплатной регистрации. После заполнения регистрационной формы программа считается активированной. Есть бесплатные варианты для Linux — **Avast! Free Antivirus for Linux** и для Mac OS — **Avast! Free Antivirus for Mac**.

- **Avast! Pro Antivirus** — условно-бесплатная версия антивируса, работает без ограничений 30 дней, затем требует файл лицензии. В отличие от бесплатной версии имеет песочницу по требованию, изолированную среду SafeZone и поддержку сканирования с помощью командной строки. Можно использовать для малых и домашних офисов.

- **Avast! Internet Security** — более совершенная условно-бесплатная версия антивируса, пакет безопасности. Также работает без ограничений 30 дней, затем требует файл лицензии. Отличается от Pro-версии наличием брандмауэра и антиспама. Также можно использовать для малых и домашних офисов.

- **Avast! Premier** — самая совершенная условно-бесплатная версия антивируса, появившаяся с восьмой версии. Отличается от Internet Security расширенным инструментом для автоматического обновления программ, возможностью удалённого доступа к ПК, а также утилитой для уничтожения данных на жёстком диске.

3.2.2. Мобильные версии

- **Avast! Free Mobile Security** — бесплатная версия антивируса для КПК на платформах Palm, Android и Windows CE. Имеет собственную Premium-версию.

3.2.3. Версии для бизнеса

- **Avast! Endpoint Protection** — платная версия антивируса для малых и домашних офисов. Помимо основных функций антивируса включает в себя функции защиты конечных точек и удалённое управление. Имеет пробную версию на 30 дней.

- **Avast! Endpoint Protection Plus** — немного более совершенная версия Endpoint Protection. Отличается наличием брандмауэра для рабочих станций и антиспама.

- **Avast! Endpoint Protection Suite** (ранее *Business Protection*) — платная версия антивируса для средних и крупных офисов, также не имеет пробной версии. Помимо основных функций антивируса включает в себя функции защиты конечных точек, защиты файловых серверов и удалённое управление.

- **Avast! Endpoint Protection Suite Plus** (ранее *Business Protection Plus*) — самая совершенная бизнес-версия антивируса, включающая функции всех вышеперечисленных продуктов.

3.2.4. Версии для серверов

- **Avast! File Server Security** — данная серверная версия ориентирована на защиту файлов, поэтому в ней отсутствуют функции защиты почтовых серверов и защиты от спама.

- **Avast! Email Server Security** — данная серверная версия ориентирована на защиту электронной почты, поэтому в ней отсутствует функция защиты файловых серверов.

3.2.5. Другие версии

- **Avast! Virus Cleaner Tool** — давно устаревший бесплатный антивирусный сканер, аналог Dr.Web Cureit! и Kaspersky AVP Tool, однако, в отличие от них, был способен удалить ограниченное число вирусов (только самые известные и опасные). Не имел резидентной защиты, поэтому не конфликтовал с другими антивирусами.

- **Avast! Windows Home Server Edition** — платная версия для домашнего сервера. Работает под Windows Home Server.

3.3. Тесты и награды

- 2006 год — Trust Award от the Secure Computing Readers как лучший антивирус[5].
- Август 2008 года — Advanced+ по рейтингу независимой тестовой компании AV-Comparatives (*англ.*).
- Февраль 2010 года — высшая награда the Platinum Performance Award от информационно-аналитического центра Anti-Malware как самый быстрый антивирусный монитор[6].
- Декабрь 2010 года — VB100 award от британского журнала Virus Bulletin.[7]
- 2010 год — avast! попал в десятку самых часто загружаемых программ на CNET Downloads и находился на втором месте[8].
- Февраль 2014 года — avast! Free Antivirus 2014 получил награду «Одобрено Anti-Malware.ru»[9].
- Апрель 2015 года — Avast! Internet Security 2015 получил награду Silver Malware Treatment Award

3.4. Примечания

[1] статистика с официального сайта

[2] Сравнение домашних версий

[3] Сравнение бизнес-ориентированных и серверных версий

[4] Нет автоматического обновления

[5] Secure Computing Readers Trust Awards

[6] Тест антивирусов на быстродействие Anti-Malware.ru

[7] AVAST wins a VB100 award and a free weekend (недоступная ссылка с 14-05-2013 (960 дней) — *история*)

[8] Top 10 Windows downloads of 2010

[9] avast! Free Antivirus 2014 получил награду «Одобрено Anti-Malware.ru»

3.5. Ссылки

- Официальный сайт (англ.)
- Официальный сайт (русскоязычный раздел)
- Награды и сертификации Avast!
- Обзор avast! Free Antivirus 8
- Обзор avast! Internet Security 6 на сайте Comss.ru

Глава 4

AVG

AVG Antivirus — антивирусная система производства чешской компании AVG Technologies, имеющая сканер файлов, сканер электронной почты и поддерживающая возможность автоматического наблюдения, а также отправки личных данных пользователя любому заинтересованному лицу. Система безопасности AVG сертифицирована всеми главными независимыми сертификационными компаниями, такими как ICSA[1][2], AV-TEST[3], Virus Bulletin, Checkmark (лаборатория West Coast Labs)[4].

AVG Antivirus существует в двух вариантах:

- бесплатная версия антивируса (AVG AntiVirus FREE)
- платная (коммерческая) версия антивируса (AVG AntiVirus и AVG Internet Security)

Основное отличие платной версии антивируса от бесплатной является:

- возможность перенастройки пользовательского интерфейса
- более гибкие настройки работы антивируса по расписанию
- возможность получения технической поддержки

AVG Antivirus — это достаточно надёжная и быстро работающая программа[5]. *Resident Shield* программы автоматически отслеживает возможное проникновение на компьютер загрузочных, исполняемых и макро-вирусов и предпринимает меры по автоматическому их удалению и лечению инфицированных файлов. *E-mail Scanner* автоматически проверяет всю входящую и исходящую почту. При включении компьютера AVG проверит оперативную память и загрузочные секторы диска, только после чего антивирус разрешит загрузку операционной системы. Далее, по завершении процесса загрузки, AVG разместит свою иконку в системной области, из которой при необходимости он может быть легко запущен.

Начиная с 15 октября 2015 года антивирус AVG Free увеличивает объем собираемых на компьютере данных. Производителю может отсылаться информация об используемых приложениях, о хакерских программах, имена подозрительных файлов, история поиска и посещений сайтов в интернете. На мобильных устройствах также отсылаются идентификаторы IMEI, IMSI и местоположение. Компания AVG оставляет за собой право продажи полученной информации компаниям-партнерам. Пользователи должны будут совершить ряд действий, чтобы отказаться от части подобной функциональности[6][7].

4.1. AVG Antivirus Pro Edition

Коммерческая Pro версия также делится на два варианта редакции: AVG Antivirus Pro и AVG Internet Security. Последняя является антивирусом со встроенными средствами защиты от интернет-атак и угроз.

4.2. Примечания

[1] AVG Internet Security в среде Windows 7 32-битная соответствовала всем требованиям при испытании антивирусного детектирования на рабочем столе/сервере

[2] AVG File Server Edition для 64-разрядной Windows 2008 — Тестирование на наличие компьютерных вирусов настольного компьютера/сервера

[3] AV-TEST — The Independent IT-Security Institute

[4] AVG Technologies — IT security, vulnerability assessment & network security

[5] Тест антивирусов на быстродействие (Март 2012 года)

[6] Компьютерра: AVG начнёт шпионить вслед за Windows

[7] AVG says it can sell your browsing data in updated privacy policy / Egadget, September 19th 2015

4.3. Ссылки

- Официальный сайт (англ.)

- Официальный сайт (рус.)

Глава 5

Avira Antivirus

AntiVir — серия антивирусных продуктов, выпускаемых немецкой компанией Avira GmbH.

5.1. Программные продукты серии

5.1.1. Avira Free Antivirus

Антивирус, бесплатный для личного использования. Продукт включает в себя резидентный монитор (который проверяет процессы при их попытке обратиться к файлам), сканер и программу автоматического или ручного обновления (в котором открывается окно с рекламным предложением приобрести коммерческую Premium-версию). Начиная с девятой версии имеется функция обнаружения рекламных программ, программ-шпионов и других вредоносных программ (ранее было только в Premium-версии).

5.1.2. Avira AntiVir Premium

Платная Premium версия персонального антивируса имеет ряд преимуществ по сравнению с бесплатной версией, наиболее значительные:

- обновления через Интернет выполняются гораздо быстрее (используются специальные серверы обновлений) и эффективнее (отсутствует рекламное окно и некоторые другие ограничения);
- защита от сайтов с вредоносным кодом;
- присутствует возможность проверки входящей и исходящей почты по протоколам POP3 и SMTP.

По результатам тестов AV-Comparatives в феврале 2009 года Avira Premium 8.2 обнаружила 99,7 % вирусов (второе место), но получила 2 звезды безопасности из-за того что заняла восьмое место в тесте на ложные срабатывания, а также заняла четвёртое место в тесте на скорость сканирования[1].

5.1.3. Avira Internet Security

Пакет безопасности отличается от Premium тем, что были добавлены персональный Firewall, анти-спам, родительский контроль (блокировка сайтов, нежелательных для просмотра детьми), игровой режим.

5.1.4. Avira Professional Security

Предназначен для защиты рабочих станций при использовании их в бизнесе. Он обладает всеми возможностями Avira AntiVir Premium и помимо этого защищает компьютеры в сети.

5.1.5. Другие продукты серии

- **AntiVir Server, AntiVir MailServer** и **AntiVir ProxyServer** — защищают серверы данных, почтовые и прокси-серверы соответственно. Стоимость каждого из них составляет от €235 до десятков тысяч евро в зависимости от количества пользователей (от 10), времени действия лицензии (1, 3 или 5 лет) и уровня технической поддержки.[2]
- **AntiVir Mobile** — несуществующий ныне антивирус для КПК и смартфонов под управлением Windows Mobile и Symbian OS. На дату ноябрь 2011 г. продажа продукта прекращена, поддержка прекращена 31 декабря 2011 года.
- **AntiVir Free Android Security** — приложение для платформы Android, которое поможет найти устройство в случае потери.
- **AntiVir Free Mac Security** — бесплатный антивирус для защиты пользователей макинтош.

5.2. Награды

- Platinum Performance Award On-Demand Scanning за февраль 2010 г. от Anti-Malware.ru[3]

- Gold Parental Control Award за декабрь 2012 г. от Anti-Malware.ru[4]

5.3. Примечания

[1] Anti-Virus Comparative No. 21, February 2009. AV-Comparatives e.V.. Проверено 30 мая 2009. Архивировано из первоисточника 11 марта 2012.

[2] Онлайн-магазин

[3] Тест антивирусов на быстродействие, рейтинг антивирусов, самый быстрый антивирус (февраль 2010) — Тесты и сравнения антивирусов — Anti-Malware.ru

[4] *Александр Панасенко.* Тест, сравнение интернет-фильтров для детей - родительских контролей (декабрь 2012) - Тесты и сравнения антивирусов. *Anti-Malware.ru* (20 декабря 2012). Проверено 21 января 2013. Архивировано из первоисточника 21 января 2013.

5.4. Ссылки

- Официальный сайт Avira на русском
- Avira AntiVir 9, softreview.com.ua, 23 марта 2009 г

Глава 6

BWMeter

BWMeter — программа для управления передачей информации по сети. С её помощью можно отображать в виде графиков загрузку сетевого канала, ограничивать скорость сетевых соединений и собирать детальную статистику по передаваемым пакетам данных.

6.1. Возможности программы

- *Обработка трафика*. Весь трафик, обрабатываемый программой, проходит через набор настраиваемых фильтров. Каждый такой фильтр выделяет часть потока из общего трафика для дальнейшей обработки. Критериями, по которым происходит выделение, являются: направление трафика (загрузка или отдача), адреса отправителя и получателя (IP-адрес, MAC-адрес, доменное имя), сетевой протокол, порт, текущие время и дата и имя прикладной программы, работающей с данными.

- *Визуализация трафика*. Выделенный фильтром поток данных можно визуализировать в виде графика в отдельном окне программы. Визуальное представление каждого графика поддаётся гибкой настройке: можно указать точное расположение окна, визуальный стиль графика (цвет, шрифт, сглаживание), интервал линий сетки, условия видимости окна, интервал обновления и многое другое.

- *Сбор статистики*. Учёт передаваемых данных может производиться как автоматически (на протяжении всего времени работы программы), так и интерактивно (с участием пользователя). Собранная автоматически статистика доступна для просмотра в виде таблицы, формируемой на основе выбранного фильтра и указанного временного интервала. Динамический сбор данных позволяет сформировать список проходящих через фильтр сетевых пакетов и сводную таблицу скоростей и объёмов переданных данных в заданный пользователем промежуток времени.

- *Уведомления*. Программа позволяет уведомлять пользователя о наступлении определённых событий: при достижении объёма загрузки/отдачи указанного значения, при пересечении скорости передачи данных заданного значения либо каждый раз после передачи определённого количества данных. Доступны несколько типов уведомлений: проигрывание звука, запуск программы, вывод сообщения на экран либо отправка электронной почты.

- *Удалённое управление*. Эта возможность позволяет просматривать активность фильтров и собирать статистику с других компьютеров сети, на которых установлена программа.

6.2. Примечания

[1] BWMeter Version History (англ.)

6.3. Ссылки

- *Сергей и Марина Бондаренко.* Программы учета сетевого трафика. 3DNews (1 февраля 2006). Проверено 30 июля 2010.

- *Alien.* Мониторинг трафика: BWMeter v.5.2.4. iXBT.com (15 июля 2010). Проверено 30 июля 2010. Архивировано из первоисточника 4 мая 2012.

Глава 7

Cisco ASA

Cisco ASA (Adaptive Security Appliance) — серия аппаратных межсетевых экранов, разработанных компанией Cisco Systems.

Является наследником следующих линеек устройств:

- Межсетевых экранов Cisco PIX;
- Систем обнаружения вторжений Cisco IPS 4200;
- VPN-концентраторов Cisco VPN 3000.

Так же как и PIX, ASA основаны на процессорах x86. Начиная с версии 7.0 PIX и ASA используют одинаковые образы операционной системы (но функциональность зависит от того, на каком устройстве она запущена).

Функциональность зависит от типа лицензии, который определяется введенным серийным номером.

Интерфейс командной строки напоминает (но не повторяет) интерфейс Cisco IOS. Управлять устройством можно через telnet, SSH, веб-интерфейс либо с помощью программы ASDM.

7.1. Возможности

- Межсетевое экранирование с учетом состояния соединений;
- Глубокий анализ протоколов прикладного уровня;
- Трансляция сетевых адресов;
- IPsec VPN;
- SSL VPN (подключение к сети через веб-интерфейс);
- Протоколы динамической маршрутизации (RIP, EIGRP, OSPF).

ASA не поддерживают протоколы туннелирования (такие, как GRE). Поддержка Policy-based routing введена в ОС версии 9.4.

7.2. Аппаратное обеспечение

7.3. Сравнение производительности

7.4. Примечания

[1] Cisco ASA Model Comparison page. Проверено 15 мая 2008. Архивировано из первоисточника 23 июля 2012.

7.5. Ссылки

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500 Models Comparison
- Cisco TAC Security Podcast - ASA troubleshooting information
- ASA Simulator
- Cisco ASA 5505 Basic Configuration
- Cisco ASA 5510 Basic Configuration

Глава 8

Comodo Firewall

Comodo Firewall — бесплатный персональный файервол компании Comodo для Microsoft Windows XP, Vista, Windows 7 и Windows 8. Comodo Firewall входит в состав Comodo Internet Security[2].

8.1. Возможности программы

1. Проактивная защита;
2. Защита от интернет-атак;
3. Защита от переполнения буфера;
4. Защита от несанкционированного доступа;
5. Защита важных системных файлов и записей реестра от внутренних атак;
6. Обнаружение переполнения буфера, которое происходит в HEAP памяти;
7. Обнаружение нападений ret2libc;
8. Обнаружение разрушенных/плохих SEH цепочек.

8.2. Особенности программы

Проактивная защита включает в себя HIPS (англ. *Host Intrusion Prevention Systems*) — система отражения локальных угроз. Задачей HIPS является контроль за работой приложений и блокировка потенциально опасных операций по заданным критериям.

8.3. Позиции в рейтингах файрволлов

На 20 января 2010 года, на сайте matousec.com, посвящённом проблемам защиты персонального компьютера программами класса Firewall, Comodo Firewall Pro 3.12.111745.56 занял первое место и получил оценку «Отлично»[3].

Тесты сайта «Firewall Challenge» от 30 марта 2008 года выдвинули Comodo Firewall версии 3.0 на первое место. Для теста компания Comodo предоставила последнюю версию сетевого экрана Comodo Firewall Pro 3.0.21.329, в которой производитель по словам представителей компании решил наиболее острые проблемы версии 3.0. Первое место Comodo Firewall поделил с программой Online Armor версии 2.1.0.119, которая в предыдущем рейтинге также занимала первое место.

В тесте HIPS на предотвращение проникновения в ядро Microsoft Windows от 20 апреля 2009 года Comodo Firewall также поделил первое место с программой Online Armor[4].

8.4. Примечания

[1] https://forums.comodo.com/news-announcements-feedback-cis/comodo-internet-security-8204674-with-win10-support-is-released-t112353-0.html

[2] Бесплатный Firewall + Antivirus Comodo!

[3] Results and comments — www.matousec.com (англ.)

[4] Тест HIPS на предотвращение проникновения в ядро Microsoft Windows

8.5. Ссылки

- Сайт компании Comodo
- Форум о программных продуктах Comodo
- Результаты тестов на www.matousec.com

Глава 9

Comodo Internet Security

Comodo Internet Security — это программный комплекс, состоящий из антивируса и персонального файрвола, а также песочницы, системы предотвращения вторжений HIPS и виртуальной среды «Virtual Kiosk» (новый компонент пакета, начиная с 6 версии) для Microsoft Windows XP, Vista, Windows 7 и Windows 8[2].

Компоненты установочного пакета Comodo AntiVirus и Comodo Firewall могут быть установлены отдельно и использоваться как самостоятельные продукты.

Comodo Internet Security (CIS) может быть использован безвозмездно (бесплатно) как для коммерческого, так и личного использования[3].

9.1. Возможности программы

- Проактивная защита.
- Защита от интернет-атак.
- Защита от переполнения буфера.
- Защита важных системных файлов и записей реестра от внутренних атак.
- Использование технологии Sandbox (песочница).
- Использование «облачных технологий».
- Полноценная виртуальная среда Virtual Kiosk.
- Очистка заражённых компьютеров с помощью Comodo Cleaning Essentials.
- Отправка любого количества файлов на анализ в Comodo.
- Встроенный диспетчер задач KillSwitch, ранее входивший в Comodo Cleaning Essentials.
- Создание диска восстановления Comodo Rescue Disk.
- Технология поведенческого анализа Viruscope.
- Веб-фильтрация.

9.2. Особенности программы

Особенностью пакета является гибкость настройки[4] — от автоматического принятия решений продуктом и оповещения об этом пользователя до полного контроля пользователя над действиями модулей продукта и принятия решений исходя из запросов и собственных предпочтений.

9.2.1. Особенности дистрибутива

В состав дистрибутива Comodo Internet Security входят:

- Браузер Chromodo (ранее известный как Comodo Dragon и написанный на коде Chromium)
- Comodo Antivirus;
- Comodo Firewall;
- Comodo Geekbuddy.

9.2.2. HIPS (Defense+)

Проактивная защита включает в себя HIPS — систему отражения локальных угроз, задачей которой является контроль за работой приложений и блокировка потенциально опасных операций по заданным критериям, а также в автоматическом режиме (поведенческий анализ) изоляция нежелательного или подозрительного объекта в «песочнице».

9.2.3. GeekBuddy

GeekBuddy — служба технической поддержки продуктов компании Comodo Group доступная пользователям, оплатившим использование продуктов Comodo и получивших лицензионный ключ (Comodo Internet Secutity PRO и иных продуктов), в пробном режиме действует 60 дней. Техническая поддержка осуществляется на английском языке круглосуточно.

9.2.4. Особенности версии 7.x

В 7-й версии Comodo Internet Security были введены следующие улучшения и изменения:

- Viruscope — система, позволяющая проводить динамический анализ поведения запущенных процессов и вести запись их активности. Viruscope контролирует деятельность процессов, запущенных на вашем компьютере и предупреждает вас, если они пытаются выполнить подозрительные действия;
- новый раздел фильтрации веб-сайтов дает пользователям способ разрешить или запретить доступ к определенным онлайн-ресурсам;
- папки с защищенными данными — функция, которая делает важные файлы полностью невидимым для программ, работающих в песочнице;
- возможность смены темы оформления.

9.3. Позиции в рейтингах

9.3.1. Тесты сайта matousec.com

На сайте matousec.com Comodo Internet Security 4.0.141842.828 занял первое место как среди бесплатных программ, так и в общем зачёте с результатом 100 % и оценкой «Excellent»[7][8]

9.3.2. Тесты сайта Anti-Malware.ru

- В тесте на способность системы HIPS защитить ядро Windows в апреле 2009 года Comodo Internet Security 3.8.65951.477 занял первое место, пройдя 9 тестов из 9[9].
- В тесте антивирусов на защиту от новейших (Zero-day) вредоносных программ в ноябре 2009 года Comodo Internet Security 3.9 занял третье место и получил награду Gold Zero-day Protection Award[10].
- В тесте самозащиты антивирусов на платформе x64 в январе 2011 года Comodo Internet Security 5.0 занял четвёртое место и получил награду Gold Self-Protection Award[11].
- В тесте файрволов на защиту от внутренних атак в сентябре 2011 года (в тестировании принимали участие 22 программы класса Internet Security) Comodo Internet Security 5.5.64714.1383 занял первое место на максимальных настройках и второе на стандартных, заслужив награду Platinum Firewall Outbound Protection Award. При настройках по умолчанию Comodo Internet Security обошёл продукты от известных производителей, настроенных по наиболее строгому варианту[12].
- В тесте файрволов на защиту от внутренних атак в июле 2013 года (в тестировании принимала участие 21 программа класса Internet Security) Comodo Internet Security 6.1.276867.2813 занял первое место на стандартных и первое на максимальных настройках, заслужив награду Platinum Firewall Outbound Protection Award[13].

9.4. Примечания

[1] https://forums.comodo.com/news-announcements-feedback-cis/comodo-internet-security-8204674-with-win10-support-is-released-t112353-0.html

[2] Antivirus for Windows 8

[3] Заявление разработчиков на официальном форуме

[4] CIS v.6 Справка-онлайн (англ.)

[5] Результаты тестов Proactive Security Challenge

[6] Результаты тестов Proactive Security Challenge 64

[7] Proactive Security Challenge (англ.)

[8] Proactive Security Challenge 64 (англ.)

[9] Тест HIPS антивирусов на предотвращение проникновения в ядро Microsoft Windows

[10] Тест антивирусов на защиту от новейших (Zero-day) вирусов, троянов, шпионских программ>

[11] Тест самозащиты антивирусов на платформе x64

[12] Тест фаерволов на защиту от внутренних атак

[13] Тест фаерволов на защиту от внутренних атак

9.5. Ссылки

- Страница программы на официальном сайте (англ.)

Глава 10

Deep packet inspection

Deep Packet Inspection (сокр. **DPI**, также **complete packet inspection** и **Information eXtraction** или **IX**) — технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. В отличие от брандмауэров, Deep Packet Inspection анализирует не только заголовки пакетов, но и полное содержимое трафика на уровнях модели OSI со второго и выше. Deep Packet Inspection способно обнаруживать и блокировать вирусы, фильтровать информацию, не удовлетворяющую заданным критериям.[1]

Deep Packet Inspection может принимать решение не только по содержимому пакетов, но и по косвенным признакам, присущим каким-то определённым сетевым программам и протоколам. Для этого может использоваться статистический анализ (например статистический анализ частоты встречи определённых символов, длины пакета и т. д.).

Deep Packet Inspection часто используются провайдерами для контроля трафика, а иногда и для блокировки некоторых приложений, таких как BitTorrent. С помощью Deep Packet Inspection можно определить, какое приложение сгенерировало или получает данные, и на основании этого предпринять какое-либо действие. Помимо блокирования, Deep Packet Inspection может собирать подробную статистику соединения каждого пользователя по отдельности. Также, при помощи quality of service Deep Packet Inspection может управлять скоростью передачи отдельных пакетов, подняв её или, напротив, уменьшив. По мнению некоторых Интернет-провайдеров, Deep Packet Inspection позволяет сдерживать приложения, забивающие Интернет-канал, изменять приоритеты передачи различных типов данных, например, ускоряя открытие Интернет страниц за счёт уменьшения скорости загрузки больших файлов. Кроме того, Deep Packet Inspection способно обнаруживать среди общего потока трафика кусочки, соответствующие компьютерным вирусам и блокировать их, повышая, таким образом, безопасность сети. Иногда Deep Packet Inspection используется в больших корпорациях для предотвращения случайных утечек данных, а также для защиты от отправки по e-mail внутренних защищённых файлов.

10.1. История

Первые брандмауэры могли быть реализованы двумя способами.

В первом способе прокси-сервер защищал внутреннюю локальную сеть от доступа из внешнего мира. Прокси-сервер проверяет, удовлетворяют ли сетевые пакеты заданным критериям. После этого либо отсеивает их, либо пересылает дальше. Такой способ использовался традиционно, так как он снижает риски, что кто-либо сможет воспользоваться уязвимостями протокола.

Во втором способе брандмауэром использовалась программа, осуществляющая фильтрацию сетевых пакетов по наборам правил. Такие программы получили название фильтрующих брандмауэров. Фильтрующий брандмауэр способен блокировать пакеты, не удовлетворяющие некоторым простым правилам, таким как IP источника, IP назначения, порт источника, порт назначения. Такие пакетные фильтры являются наиболее быстро работающим типом брандмауэров, так как делают совсем немного вычислений. Простота реализации позволяет делать такой брандмауэр в виде микросхемы.

С самого начала прокси-сервера были признаны более безопасными, нежели пакетные фильтры, поскольку они более детально осуществляли проверку пакетов.[2]

Эволюция брандмауэров на основе прокси-серверов привела к появлению первых программ Deep Packet Inspection. Они были созданы в целях устранения сетевых проблем и для блокирования вирусов, а также в целях защиты от DoS-атак. Первоначально компьютеры, на которых был установлен Deep Packet Inspection, не были достаточно мощными, чтобы контролировать весь Интернет-трафик пользователей в режиме реального времени.

Через некоторое время, когда появилась возможность работы программ Deep Packet Inspection в

режиме реального времени, они использовались интернет-провайдерами в основном для организации целевой рекламы и уменьшения заторов в сети. Сегодня же Deep Packet Inspection способно на много большее, чем просто обеспечивать безопасность. Интернет-провайдеры получили возможность контролировать проходящий трафик любого своего клиента. Наличие инструментов для выборочного блокирования трафика даёт интернет-провайдерам возможность добавлять дополнительные платные услуги и получать с этого дополнительный доход, хотя по сути, это нарушает сетевой нейтралитет.[3] В настоящий момент в некоторых странах интернет-провайдеры обязаны выполнять фильтрацию в соответствии с законодательством страны. Программы Deep Packet Inspection иногда используют для обнаружения и блокирования трафика, содержащего незаконные материалы или нарушающего авторские права[4]

В последнее время объём проходящего трафика заметно возрос. Начинает вновь возникать проблема, что компьютеры не справляются с анализом всего трафика в реальном времени или же стоимость компьютеров будет слишком велика. Однако современные технологи уже позволяют сделать полнофункциональный Deep Packet Inspection в виде специального роутера.[5] Так же набирают популярность программные решения, которые устанавливаются на доступные аппаратные платформы.[6]

10.2. Пример работы Deep Packet Inspection

10.2.1. Идентификация протокола транспортного уровня сетевой модели OSI

В структуре пакета протокола IPv4 выделен специальный байт для указания номера протокола транспортного уровня. Им является десятый байт от начала заголовка IPv4 пакета. Например: номер равняется шести — для TCP протокола, номер равняется семнадцати — для UDP протокола.

В структуре пакета IPv6 также существует специальная область, в которой находится аналогичный идентификатор протокола транспортного уровня. Эта область носит название Next Header. [7]

10.2.2. Идентификация BitTorrent

Клиенты BitTorrent соединяются с трекером по протоколу TCP. Для того, чтобы обнаружить среди всего трафика TCP такие пакеты, достаточно проверить, что содержимое данных TCP пакета со второго байта совпадает с «BitTorrent protocol»[8]

10.2.3. Идентификация HTTP

Для идентификации HTTP протокола достаточно проверить, что пакет является TCP, и содержимое этого TCP пакета начинается с одной из следующих команд: «GET», «POST», «HEAD». Кроме того, после команды должен стоять пробел, а также через некоторый промежуток должен встретиться текст «HTTP/». Если всё это выполняется, то этот пакет несёт в себе HTTP запрос.[8]

10.2.4. Идентификация RTSP

Для того, чтобы обнаружить среди всего трафика пакеты RTSP, достаточно убедиться, что пакет является TCP и содержимое этого TCP пакета начинается с одной из следующих команд: «OPTIONS», «DESCRIBE», «ANNOUNCE», «PLAY», «SETUP», «GET_PARAMETER», «SET_PARAMETER», «TEARDOWN». После команды должен стоять пробел. Также, через некоторый промежуток должен встретиться текст «RTSP/».[8]

10.3. Для чего применяется DPI?

10.3.1. Реализация QoS

С точки зрения эксплуатации, оператор может контролировать утилизацию подключенных через DPI каналов на уровне приложений. Раньше он решал задачи реализации QoS (Quality of Service) исключительно средствами построения очередей на основании маркировки трафика служебными битами в заголовках IP, 802.1q и MPLS, выделяя наиболее приоритетный трафик (разного рода VPN'ы, IPTV, SIP и т. д.) и гарантируя ему определённую пропускную способность в любой момент времени. Трафик типа Best Effort, к которому относится весь интернет трафик домашних абонентов (HSI — High Speed Internet), оставался фактически без контроля, что давало возможность тому же Bittorrent забрать себе всю свободную полосу, что, в свою очередь, вело к деградации любых других веб-приложений. С использованием DPI у оператора появляется возможность распределить канал между различными приложениями. К примеру, в ночные часы разрешить трафику Bittorrent забирать себе больше полосы, чем днём, в часы-пик, когда в сети ходит большое количество другого веб-трафика. Другая популярная мера у многих мобильных операторов — блокировка Skype-трафика, а также любых видов SIP-телефонии. Вместо полной блокировки оператор может разрешать работу данных протоколов, но на очень низкой скорости с соответствующей деградацией качества предоставления сервиса у конкретного приложения, чтобы вынудить пользователя платить за услуги традици-

онной телефонии, либо за специальный пакет услуг, разрешающий доступ к VoIP-сервисам.

10.3.2. Subscriber Management

Важным моментом является то, что правила, на основании которых выполняется шейпинг/блокировка, могут быть заданы посредством двух основных базисов — per-service или per-subscriber. В первом случае простейшим образом оговаривается, что конкретному приложению позволяется утилизировать определённую полосу. Во втором привязка приложения к полосе осуществляется для каждого подписчика или группы подписчиков независимо от других, что производится через интеграцию DPI с существующими OSS/BSS системами оператора. То есть можно настроить систему таким образом, что подписчик Вася, который за неделю накачал торрентов на 100 гигабайт, до конца месяца будет ограничен по скорости скачивания этих же торрентов на уровне 70 % от купленного им тарифа. А у подписчика Пети, который купил дополнительную услугу под названием «Skype без проблем», трафик приложения Skype не будет блокироваться ни при каких условиях, но любой другой — легко. Можно сделать привязку к User-Agent и разрешить браузинг только при помощи рекомендуемых браузеров, можно делать хитрые редиректы в зависимости от типа браузера или ОС. Иными словами, гибкость тарифных планов и опций ограничена лишь здравым смыслом. Если же речь идёт о трафике мобильных операторов, то DPI позволяет контролировать загрузку каждой базовой станции в отдельности, справедливо распределяя ресурсы БС таким образом, чтобы все пользователи остались довольны качеством сервиса. Большинство производителей пакетного ядра EPC (Evolved Packet Core) для LTE интегрирует в свой PDN-GW функционал DPI, приспособленный для решения задач мобильных операторов.

10.4. Программное обеспечение

Hippie (Hi-Performance Protocol Identification Engine) — реализация Deep Packet Inspection для Linux с открытым исходным кодом на C.[8]

L7-filter — ещё одна реализация Deep Packet Inspection для Linux с открытым исходным кодом на C, ориентированная на классификацию данных седьмого уровня модели OSI.[9]

SPID (Statistical Protocol IDentification) — реализация Deep Packet Inspection для Windows с открытым исходным кодом на C#. Идентифицирует протокол седьмого уровня модели OSI с помощью статистического анализа трафика.[10]

10.5. Использование Deep Packet Inspection в России и мире

Deep Packet Inspection способно изменять данные в пакетах. В Соединённых Штатах Америки и Великобритании Deep Packet Inspection часто используется для генерации рекламы, основанной на поведении абонентов. Таким образом реализуется так называемый целевой маркетинг.[11]

Основные сотовые операторы России внедрили DPI в 2009 (Мегафон, оборудование Huawei), 2010 (МТС, Cisco) и 2011 (Билайн, Procera) годах. Они могут использовать DPI в том числе для подавления peer-to-peer и VoIP сервисов.[12][13] Ростелеком планирует внедрить DPI для мобильного интернета в 2014 году.

Кипрская компания *iMarker* (зарегистрирована и действует по законам Республики Кипр[14]) с начала 2010 года предлагала интернет провайдерам бесплатную установку DPI-систем (Gigamon, Xterica) с целью таргетирования интернет-рекламы. Подобная система получает информацию обо *всех* сайтах, посещаемых пользователями и на базе этого может предложить ему персонализированную рекламу. По данным газеты Ведомости, такая система уже установлена у 11 операторов, включая 4 региональных филиала Ростелекома; общий охват оценивался основателем компании на конец 2013 года в 12 % российской интернет-аудитории[15][16][17][18]. Позже iMarker фактически стал частью американской компании Phorm, предлагающей подобные услуги для европейских интернет-провайдеров.

В России тенденции к внедрению Deep Packet Inspection у интернет-провайдеров также связаны с федеральным законом № 139 о внесении изменений в закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (вступил в силу 1 ноября 2012 года). Большинство интернет-провайдеров обеспечивают блокирование сайтов, занесённых в чёрный список, основываясь только на IP адресах этих сайтов. Но некоторые провайдеры могут блокировать выборочные URL-адреса, если у них используется Deep Packet Inspection для анализа HTTP-запросов.[19][20]. К шифрованным соединениям (HTTPS) применение техники DPI затруднено.

Одним из препятствий обязательного применения DPI-технологий российскими провайдерами для блокировки запрещенных сайтов стала дороговизна подобных решений, а также наличие более дешевых альтернатив для фильтрации по URL-адресу с целью исполнения закона. [21]

Основные доводы противников использования Deep Packet Inspection — противоречие статье 23[*источник не указан 369 дней*] Конституции РФ("..право на неприкосновенность частной жизни, личную и семейную тайну..” и "..право на тайну переписки,

телефонных переговоров, почтовых, телеграфных и иных сообщений..”), а также правилам конфиденциальности. Также Deep Packet Inspection по своей сути нарушает сетевой нейтралитет.[22]

10.6. Примечания

[1] Краткий обзор DPI — Deep Packet Inspection

[2] What is «Deep Inspection»?

[3] Deep packet inspection: the end of the internet as we know it?

[4] The End of the Internet?

[5] Cisco: Application Visibility and Control (AVC)

[6] VAS Experts - Обзор компонент

[7] Assigned Internet Protocol Numbers: Protocol Numbers

[8] Sourceforge.net: hippie

[9] Официальный сайт l7-filter

[10] Sourceforge.net: spid

[11] Profiling the Profilers: Deep Packet Inspection and Behavioral Advertising in Europe and the United States

[12] Роман Дорохов, Российская iMarker научилась зарабатывать на чужом интернет-трафике. Компания бесплатно ставит операторам систему анализа трафика, собирает данные о поведении пользователей и продает их рекламодателям // Ведомости, 28.08.2013: "С помощью DPI операторы могут вводить новые тарифные планы — например, делать бесплатным доступ к собственным сайтам или резко снижать скорость доступа в интернет пользователю после того, как тот использовал выделенный ему суточный лимит трафика. Поэтому первыми в России DPI начали внедрять сотовые операторы: «Мегафон» — в 2009 г., МТС — в 2010 г. и «Вымпелком» — в 2011 г.”

[13] Интернет-фильтрация в России: еще и слежка // Forbes, 02.11.2012: "К лету 2012 года все три национальных оператора сотовой связи уже поставили DPI на своих сетях: Procera стоит в «Вымпелкоме», Huawei используется в «Мегафоне», а МТС закупил DPI от Cisco. ... траффик-шейпинг,... с помощью DPI мобильные операторы получили возможность подавлять определенные сервисы — прежде всего, торренты, peer-to-peer протоколы или Skype”

[14] http://www.imarker.ru/static/partner_offer.pdf - Оферта iMarker: "предложение Компании «VSP VIRTUAL SERVICES PROVIDER» Ltd. (адрес: Iasonos, 5, Palodeia, P.C. 4549, Limassol, Cyprus, далее – «IMARKER»)"

[15] Роман Дорохов, Российская iMarker научилась зарабатывать на чужом интернет-трафике. Компания бесплатно ставит операторам систему анализа трафика, собирает данные о поведении пользователей и продает их рекламодателям // Ведомости, 28.08.2013: "Он предлагает заработать на адресной интернет-рекламе с помощью систем контроля и управления трафиком DPI (Deep Packet Inspection). Эта система умеет отслеживать любой незашифрованный трафик пользователей — от электронной переписки и звонков до изображений и личных сообщений в соцсетях. ... iMarker работает с января 2010 г., ее систему установили 11 операторов (в том числе в четырех филиалах «Ростелекома») и она собирает данные по 12% пользователей рунета, говорит Берлизев.”

[16] iMarker зарабатывает на трафике 12% пользователей рунета // theRunet, 28 августа 2013

[17] Российские провайдеры собирают для рекламщиков данные о поведении пользователей // Компьютерра, Андрей Письменный 29 августа 2013

[18] iMarker Selects Gigamon® for Deployment With Its TargetJ-Based Advertising Platform - Пресс-релиз Gigamon, 2011/05/03: “VSP iMarker ... target-based advertising service platform, which is deployed in several telecom operators’ networks across Russian Federation, including OJSC Svyazinvest regional telco companies (MRK).”

[19] inopressa: В России вступил в силу закон об интернет-цензуре - по материалам Die Presse Russland: Gesetz für Internet-Zensur in Kraft, 05.11.2012

[20] Интернет-фильтрация в России: еще и слежка // Forbes, 02.11.2012: "Самое опасное в новой всероссийской системе блокировки интернет-ресурсов ... операторам придется закупить и установить технологию DPI (глубокого чтения пакетов). .. реестр требует ограничения доступа к ресурсам .. по указателям отдельных страниц (URL), для блокировки которых наиболее эффективна эта технология. "

[21] Евгений Тетенькин: Блокировка сайтов не должна травмировать Рунет // CNews Безопасность, 2012/11/30

[22] What Is Deep Packet Inspection?

10.7. Литература

- Requirements for deep packet inspection in Next Generation Networks (Y.2770) // ITU-T

10.8. Ссылки

- Краткий обзор технологии DPI — Deep Packet Inspection (рус.)

Глава 11

Fortinet

Fortinet — американская компания, специализирующаяся на программно-аппаратных комплексах сетевой безопасности (*security appliances*) и UTM-решениях (англ. Unified threat management).

Компания Fortinet была основана в 2000 году Кеном Кси, основателем и бывшим президентом NetScreen, и является публичной компанией (код NASDAQ — FTNT). Компания Fortinet занимает наибольшую долю рынка среди UTM-решений, что неоднократно подтверждалось IDC.[2], занимает 3-4 место в мире по ежегодному объёму продаваемых устройств сетевой безопасности[3][4][5][6]. Флагманский продукт компании Fortinet продается под торговой маркой FortiGate.

Fortinet — это международная компания, головной офис находится в Саннивейле, Калифорния. Fortinet распространяет свои продукты и сервисы, используя партнерский канал продаж. У Fortinet более 10,000 партнеров по всему миру.

В 2012—2013 годах капитализация компании превысила 3 млрд. US$, что позволяет сравнивать ее с компаниями индекса S&P 500[7][8]. По отзыву аналитиков компании Merrill Lynch, хорошие технологии, разработанные в Fortinet, специализация и общая оценка продуктов компании, позволяют поставить ее в верхнем конце шкалы; однако конкуренция в данной области высока, и компания находится под постоянной угрозой того, что существующие или новые конкуренты могут сократить разрыв в технологиях, специализации и общей оценке[9].

11.1. Обзор продуктов

Fortinet предлагает шлюзы безопасности и другие продукты, характеризующиеся высокопроизводительными ASIC-процессорами, интегрированной комплексной защитой и постоянными обновлениями. Продукты Fortinet рассчитаны на использование организациями любого размера (SMB, Enterprise, сервис-провайдеры, телекомы). Доступны такие продуктовые линейки:

11.1.1. FortiGate

Шлюз безопасности FortiGate-100D

Шлюз комплексной безопасности FortiGate обеспечивает разнообразную функциональность, необходимую для комплексных UTM-решений. Fortinet на протяжении пяти лет (2009—2013) находится в группе лидеров в Магическом Квадранте компании Gartner по UTM решениям[10][11]. FortiGate является флагманским продуктом в линейке продуктов сетевой безопасности Fortinet. Обеспечиваемая шлюзом функциональность:

- Маршрутизатор
- Межсетевой экран (Next-Generation Firewall)
- IPSec и SSL VPN
- WAN оптимизация
- Traffic shaping
- Контроль доступа к сети (NAC)
- Контроль приложений
- Предотвращение утечки данных (DLP)
- Контроль уязвимостей
- Антиспам (AS)
- Антивирус (AV)
- Веб-фильтр
- Система предотвращения вторжений (IPS)
- WiFi-контроллер

11.1.2. Безопасность и доступность серверов и веб-приложений

- **FortiDDoS** — специализированное решение для защиты от DDoS-атак
- **FortiWeb** — защита веб-приложений
- **FortiBalancer**
- **FortiADC**

11.1.3. Построение и защита беспроводной сети

- **FortiAP** — беспроводные точки доступа[12]
- **FortiWiFi** — шлюз безопасности FortiGate со встроенной беспроводной точкой доступа

11.1.4. Усиление аутентификации

- **FortiAuthenticator** — серия устройств безопасной аутентификации FortiAuthenticator работает вместе с токенами двухфакторной аутентификации FortiToken, обеспечивая защищенный удаленный доступ к сети.
- **FortiToken** — токены для двухфакторной аутентификации

11.1.5. Централизованное управление и отчетность

- **FortiManager** — централизованное управление устройствами Fortinet
- **FortiAnalyzer** — собирает, анализирует и регистрирует данные о событиях с устройств сетевой безопасности Fortinet или syslog-совместимых устройств.

11.1.6. Другие специализированные решения для обеспечения безопасности

- **FortiMail** — устройства почтовой безопасности
- **FortiDB**— защита баз данных
- **FortiClient** — безопасность конечных точек
- **FortiScan** — контроль уязвимостей
- **FortiCarrier** — шлюзы безопасности для провайдеров

11.1.7. Сетевое оборудование

- **FortiSwitch** — линейка коммутаторов 1 GbE, 10 GbE и PoE
- **FortiBridge** — устройства перенаправления трафика
- **FortiDNS** — защищенные кэширующие DNS серверы
- **FortiCache**

11.1.8. IP-телефония

- **FortiVoice**
- **FortiFone**

11.1.9. Видеонаблюдение

- **FortiCam**

11.2. Исследовательский центр FortiGuard

Лаборатория FortiGuard Research Center является частью компании Fortinet и занимается исследованиями в сфере информационной безопасности и выпуском обновлений для части функциональности решений Fortinet. Филиалы исследовательского центра FortiGuard открыты в США, Канаде, Франции, Великобритании, Японии, Китае и Сингапуре. На текущий момент в лаборатории FortiGuard работает более 200 аналитиков и инженеров безопасности.

Центр выпускает широко цитируемый регулярный отчет о положении дел в сфере компьютерной безопасности (*Threat Landscape Report*). В отчете за октябрь 2011 года центр FortiGuard объявил об обнаружении первого ботнета на платформе Андроид[13]

11.2.1. Сервисы FortiGuard

- Антиспам
- Антивирус
- Система предотвращения вторжений (IPS)
- Веб-фильтр — все сайты распределены между 6 основными категориями и 78 подкатегориями (полный список категорий)
- Application firewall — на текущий момент лабораторией FortiGuard выпущены сигнатуры для 2984 приложений (полный список приложений)

11.3. Сертификаты и награды

- NSS Labs 'Recommended' Rating in 2013 Firewall Comparative Analysis[14]
- NSS Labs 'Recommended' Rating in 2012 Network Intrusion Prevention Comparative Testing[15]
- ICSA Labs Certified: Antivirus, Corporate Firewall, IPSec, NIPS, SSL-TLS and Web Application Firewall [16]
- IPv6 Ready Phase 2 [17]
- CVE-Compatible Products and Services [18]
- Common Criteria
- FIPS 140-2
- Wi-Fi Alliance [19]
- Microsoft Certification [20]
- ISO 9001:2008
- На 2013 год, занимает 25-е место в списке лучших малых компаний США (*America's Best Small Companies*), составляемом Forbes[1]
- Две награды 2014 *Network World Asia Information Management* в категориях «Фаерволл и сетевая безопасность», и «UTM-решения»[21]

11.4. См. также

11.5. Примечания

[1] Fortinet — Forbes, Октябрь 2013

[2] Fortinet Named Leader of Worldwide Unified Threat Management Market for 23rd Consecutive Quarter by Leading Market Research Firm. Fortinet.

[3] Fortinet Grows to Fourth Largest Network Security Company According to Leading Market Research Firm (англ.) — Yahoo! Finance, 25/07/2012

[4] IDC says Check Point, Fortinet gain on Cisco in security appliance market 25/6/2013

[5] Network Security Sustains Growth Momentum in First Quarter of 2014 — IDC, 09/06/2014

[6] Security Appliance Market Growth Slows in First Quarter, According to IDC — IDC, 24/06/2013

[7] Fortinet Larger Than S&P 500 Component Tenet Healthcare — Forbes, Декабрь 2012

[8] Fortinet Moves Up In Market Cap Rank, Passing Assurant — Forbes, Декабрь 2012

[9] Fortinet, SourceFire: Merrill Launches With Buy Ratings — Forbes, 15/11/2011

[10] Fortinet Positioned in the Leaders Quadrant for 2013 Unified Threat Management. Fortinet.

[11] Magic Quadrant for Unified Threat Management — Dell

[12] *Greg Masters.* Case study: Easing learning. *SC Magazine* (March 03, 2014). Проверено 25 июня 2014.

[13] Fortinet discovers the first extensible Android botnet. *InfoSecurity* (4 November 2011). Проверено 25 июня 2014.

[14] Fortinet® Earns "Recommend" Rating in NSS Labs' 2013 Firewall Comparative Analysis. Fortinet.

[15] Fortinet® Earns NSS Labs' 'Recommended' Rating in 2012 Network Intrusion Prevention Comparative Testing. Fortinet.

[16] Fortinet, Inc. | ICSA Labs

[17] IPv6 Ready Logo Program Approved List

[18] CVE - Compatible Products and Services

[19] Submit Form

[20] Windows Server Catalog

[21] Fortinet Wins Multiple Awards From Network World and Computerworld — IT Buisness, 12/06/2014

11.6. Ссылки

- **fortinet.com** — официальный сайт Fortinet
- Исследовательская лаборатория FortiGuard
- Блог компании Fortinet
- Полезные настройки Fortinet

Глава 12

Ideco ICS

Ideco ICS (англ. *Internet Control Server*, сервер управления доступом в Интернет) — программный Интернет-шлюз на ядре Linux, используемый для контроля и распределения доступа в Интернет в корпоративных и частных сетях. Компания-разработчик - "Айдеко".

12.1. Описание

Ideco ICS является комплексным Интернет-шлюзом и содержит встроенные модули[*значимость не указана 176 дней*]:

- файрволл
- почтовый сервер
- антивирус
- антиспам
- модуль DLP
- VPN-сервер
- DNS-сервер

Служит для распределения, учёта и контроля доступа в Интернет на предприятиях, в частных и провайдерских сетях. Управление интернет-шлюзом осуществляется через графический веб-интерфейс из-под любой распространенной операционной системы (Windows, Linux, Mac OS). Может поставляться с коммерческими антивирусными продуктами, например, с антивирусом Касперского или ClamAV.

Первый в России интернет-шлюз с функционалом DLP.[1]

12.2. Награды

- Премия BestSoft (журнал PC Magazine) — 2008, 2009, 2010, 2011, 2012, 2013.
- Продукт года 2010 в категории «Комплексные сетевые решения»[2]
- Best Soft 2010 по версии русского издания журнала PCmagazine[3]
- Продукт года — 2008 в категории «Системы сетевого управления»[4]
- Один из лучших программных продуктов 2009 по версии русского издания журнала PCmagazine[5]

12.3. Примечания

[1] «Айдеко»: DLP-система объединена с интернет-шлюзом

[2] Продукт года — 2010

[3] http://pcmag.ru/reviews/sub_detail.php?ID=43162 — Российское ПО 2010: инновации и достижения (рус.). PC Magazine/Russian Edition (2010-11-21). Проверено 13 августа 2011.

[4] Продукт года — 2008

[5] Лучшие программные продукты — 2009

12.4. См. также

- Интернет-шлюз
- Межсетевой экран
- Предотвращение утечек

12.5. Ссылки

- Официальный сайт продукта
- http://www.pcmag.ru/software/detail_rev.php?ID=30067 — Ideco Internet Control Server., PC Magazine Russian Edition.
- Linux Format: об Ideco ICS

- http://www.pcmag.ru/reviews/detail.php?ID=37502&phrase_id=2821939 — Лучшие программные продукты 2009 года., PC Magazine Russian Edition.

Глава 13

ipchains

Ipchains (*Linux IP Firewalling Chains*) — открытый программный проект, состоящий из встроенного в ядро Linux 2.2 средства фильтрации пакетов/межсетевого экрана (ipchains) и программ управления им (ipchains, ipchains-save, ipchains-restore). Автор проекта — Расти Расселл (en:Rusty Russell). До ipchains в Linux использовался файрволл *IPV4 firewall*, перенесённый из BSD, его утилитой управления являлся ipfwadm (переписанная утилита ipfw из BSD). В дальнейшем, в ядрах 2.4 и более новых, ipchains был заменен системой netfilter/iptables[1], созданной под руководством Расти.

В отличие от iptables, ipchains работает как stateless-firewall.

В виде патчей ipchains был доступен и для ядер серии 2.0 и 2.1. По сравнению с ipfwadm, проект ipchains позволял[2]:

- Увеличение пределов подсчёта/учёта пакетов;
- Возможность фильтрации фрагментированных пакетов;
- Поддержку большего количества сетевых протоколов;
- Возможность использования инверсии условия.

В поставку ipchains включены некоторые скрипты для упрощения миграции с ipfwadm.

13.1. Примечания

[1] netfilter/iptables project homepage (6 февраля 2009). Проверено 8 февраля 2009. Архивировано из первоисточника 4 июля 2012.

[2] *Russell, Rusty* Linux IPCHAINS-HOWTO (4 июля 2000). Проверено 8 февраля 2009. Архивировано из первоисточника 4 июля 2012.

13.2. Ссылки

- IPChains HOWTO: на TDLP и на FAQs.org

Глава 14

IPFilter

IPFilter (в основном упоминается как **ipf**) — открытое программное обеспечение; межсетевой экран и преобразователь сетевых адресов (NAT) для многих Unix-подобных операционных систем. Его автор — Даррен Рид.

IPFilter поставляется с FreeBSD, NetBSD и Solaris 10. До мая 2001 года он входил и в OpenBSD, но был исключен из-за разногласий между Тэо де Раадтом и Дарреном Ридом по лицензии на IPFilter. На первый взгляд, лицензия во многом похожа на лицензии BSD, но не позволяет распространение изменённых версий.

IPFilter может использоваться как загружаемый модуль ядра или непосредственно включён в ядро операционной системы, в зависимости от специфики ядра и пользовательских предпочтений. Документация рекомендует пользоваться загружаемым модулем, если это возможно.

Список операционных систем, поддерживающих IPFilter, включает следующие:

- IBM AIX 5.3 ML05
- BSD/OS−1.1 — 4
- FreeBSD 2.0.0 — 7.0
- IRIX 6.2, 6.5
- HP-UX 11.00
- Ядро Linux 2.4 — 2.6
- NetBSD 1.0 — 5.x
- OpenBSD 2.0 — 3.8
- OpenSolaris
- QNX 6
- Solaris 2.3 — 10
- SunOS 4.1.3 — 4.1.4
- SCO OpenServer/UnixWare
- Tru64 5.1a
- CAOS Linux NSA 1.0

14.1. См. также

- Netfilter
- Ipfw
- Pf
- NPF

14.2. Ссылки

- Домашняя страница проекта IPFilter (англ.)
- Текущая лицензия проекта IPFilter (англ.)
- Официальное руководство по настройке IPFilter в FreeBSD
- Использование IPFilter во FreeBSD
- NAT во FreeBSD с помощью IPFilter (ipnat)

Глава 15

IPFire

IPFire — свободный дистрибутив на базе Linux для создания маршрутизаторов и межсетевых экранов.

С версии 2, используется только сетевой интерфейс IPCop.

15.1. Системные требования

Модульный дизайн позволяет устанавливать и настраивать систему под заказ. Можно установить очень маленькую систему на первых поколениях процессоров Intel Pentium или современную многопроцессорную SOHO-систему.

Требования производительности зависят от сферы применения. Но минимальные требования таковы: 333 MHz CPU, 256 MB RAM и 2 сетевых интерфейса — один для соединения с Интернетом и один для локальной сети.[1]

15.2. Возможности

IPFire обслуживает пользователей не слишком знакомых с сетевыми и серверными услугами. IPFire поставляется с расширенной утилитой управления пакетами (Pakfire), которая позволяет установить на базовую систему дополнения. Менеджер пакетов также устанавливает обновления безопасности.

Основные функции:

- Прокси-сервер с контентной фильтрацией и кешем для обновлений (пример: Microsoft Windows Updates и антивирусные базы)
- Intrusion detection system (Snort) with intrusion prevention-addon «guardian»
- VPN via IPsec and OpenVPN
- DHCP-server
- Caching-nameserver
- Time server
- Wake-on-LAN (WOL)
- Dynamic DNS
- Quality of Service
- Outgoing firewall
- System monitoring and Log-Analysis

15.3. Дополнения

IPFire offers add-ons which are maintained by the development team.

Вот некоторые из них:

- Файл- и принт-сервер (Samba и CUPS, vsftpd)
- Asterisk и Teamspeak
- Video Disk Recorder (VDR)
- Почтовый сервер — Postfix, SpamAssassin, ClamAV, Amavis (amavisd-new)
- Потоковый сервер (MPD a.o.)

15.4. Портирование

IPFire был портирован на ARM архитектуру 2011. Сейчас запускается на Pandaboard, Raspberry Pi[2] и Marvell Kirkwood платформе DreamPlug.

15.5. Miscellaneous

- IPFire is part of the c't-Debian-server version 4, which was released in August 2009.

15.6. Примечания

[1] IPFire wiki page about Hardware. ipfire.org. Проверено 22 декабря 2010.

[2] [SIG-ARM] IPFire on Raspberry Pi ready to fist test

15.7. Ссылки

- Официальный сайт
- IPFire at Distrowatch
- IPFire at the CeBIT 2010 in Hannover
- IPFire on The-H online
- IPFire on LWN.net
- IPFire Video on Bóson Treinamentos — In Portuguese

Глава 16

Ipfw

ipfirewall — межсетевой экран, который поставляется с FreeBSD начиная с версии 2.0. С его помощью можно, например, подсчитывать трафик по любым разумным правилам, основывающимся на данных заголовков пакетов протоколов стека TCP/IP, обрабатывать пакеты внешними программами, прятать за одним компьютером целую сеть и т. п.[1]

Используется во многих ОС для встраиваемых систем, основанных на FreeBSD, таких как m0n0wall.

Имеется портированная версия — Wipfw для Windows 2000, Windows XP, и Windows Server 2003.

ipfw — название пользовательской утилиты (запускаемой из командной строки) предназначенной для управления системой IPFW. С её помощью администраторы создают и изменяют правила, управляющие фильтрацией и перенаправлением пакетов.

ipfw может быть подгружен как модуль, а может быть встроен в ядро.

Ipfirewall состоит из следующих компонентов:

- обработчик правил на уровне ядра, включающий систему учета пакетов
- механизм логирования
- механизм форвардинга
- ipstealth (механизм редактирования TTL полей, защита от traceroute)
- основанные на ALTQ средства управления QoS
- средства для управления множеством правил
- механизмы управления пропускной способностью
- основанная на таблице маршрутов система антиспуффинга
- счетчики пакетов
- встроенный NAT, PAT и LSNAT (начиная с FreeBSD 7)
- поддержка IPv6 (с некоторыми ограничениями)

16.1. История

Утилита ipfw впервые появилась во FreeBSD 2.0. Поддержка dummynet была добавлена позже, начиная с версии 2.2.8. Поддержка divert socket вместе с natd была добавлена начиная с версии 3.x (уточнить). Поддержка NAT на уровне ядра была добавлена начиная с версии 7.0.

16.2. Авторы

- Ugen JS Antsilevich
- Poul-Henning Kamp
- Alex Nash
- Archie Cobbs
- Luigi Rizzo

Поддержка NAT на уровне ядра была написана Paolo Pisati и впервые появилась в FreeBSD 4.0. До этого преобразование NAT осуществлялось демоном natd, пакеты которому передавались действием divert.

16.3. Описание

Настроенный брандмауэр представлен упорядоченным списком правил с номерами из диапазона 1-65535. Каждый пакет приходит с различных уровней стека протоколов, и попадая на брандмауэр поочередно сравнивается с критерием каждого правила в списке. Если совпадение найдено, то выполняется действие, закрепленное за данным правилом.

ipfw всегда содержит правило по умолчанию (с номером 65535) которое не может быть ни изменено, ни удалено. Это правило является терминальным, т.е оно применяется к пакетам, не попавшим во все предыдущие. В зависимости от конфигурации ядра это правило может выполнять действия «запретить» или «разрешить»(по умолчанию оно deny ip from any to any, что бы изменить это, в ядро нужно добавить

options IPFIREWALL_DEFAULT_TO_ACCEPT). Все остальные правила могут редактироваться администратором системы.

Существует несколько основных действий, которые могут применяться к пакетам:

- **allow** (*син.* — pass, accept, permit) — разрешить прохождение пакета. После этого действия другие правила не рассматриваются.
- **deny** (*син.* drop) — запретить (сбросить) пакет. Пакет прекращает движение по списку правил и система полностью про него забывает.
- **unreach** — запретить пакет. В отличие от deny, отправителю отправляется сообщение об ошибке по протоколу ICMP. После этого действия другие правила не рассматриваются.
- **reject** — запретить пакет, и послать отправителю «Заданный узел не найден»
- **skipto** — перейти к правилу с заданным номером, минуя все промежуточные (используется для того, чтобы избежать просмотра списка правил, условия которых заведомо не выполняются).
- **fwd** (*син.* forward) — перенаправление пакета (используется для организации «transparent-proxy»; а также для маршрутизации пакетов по IP-адресу источника или любым другим признакам, не обрабатываемым обычной маршрутизацией).
- **divert** — передать пакет на анализ пользовательскому приложению, которое может изменить пакет и вернуть его в firewall (возвращённый пакет будет передан следующему правилу) либо уничтожить пакет.
- **tee** — аналогичен divert, за исключением того, что на анализ передается копия пакета (чаще всего используют для подсчета трафика).
- **pipe**, **queue** — прохождение пакета через «канал» или «очередь» dummynet (shaping). Используется для ограничения пропускной способности и внесения задержек в прохождение пакетов.

16.4. Включение во FreeBSD

При установке системы FreeBSD стандартными средствами, ipfw по умолчанию не включён. Поддержка может быть выполнена либо включением кода ipfw в ядро (добавлением опций и перекомпиляцией ядра с последующей перезагрузкой системы), либо (в любой момент после загрузки системы) подключением одноимённых модулей (доступно в последних версиях системы). Загрузка процессора меньше при включении ipfw в ядро, однако, это заметно лишь при большом количестве обрабатываемых пакетов и правил.

Если вы хотите использовать IPFW, то вам необходимо пересобрать ядро с опцией:

options IPFIREWALL

По умолчанию в IPFW встроено неудаляемое правило "всем всё запрещено", которое имеет наибольший номер и потому будет обрабатываться после всех правил, внесённых администратором системы. При некоторых ошибочных действиях администратора система может оказаться закрытой от любого доступа по сети, и администратору потребуется доступ к консоли; чтобы заменить это правило на "всем всё разрешено", надо добавить опцию

options IPFIREWALL_DEFAULT_TO_ACCEPT

Если вы хотите использовать NAT (посредством демона natd), то вам необходимо *добавить* опцию:

options IPDIVERT

Если вы хотите использовать NAT уровня ядра, то вам необходимо *добавить* опции:

options LIBALIAS options IPFIREWALL_NAT

Если вы хотите использовать pipe/queue, то вам необходимо *добавить* опцию:

options DUMMYNET

Включение ipfw через загрузку модулей ядра выполняется (суперпользователем) командами

kldload ipfw kldload ipdivert kldload dummynet

соответственно.

16.5. Как строить правила

Общий формат для построения правил:

ipfw [prob *match_probability*] action [log *logamount number*] *proto* from *src* to *dst* [*options*]

ipfw add 00001 allow icmp from any to any
: разрешить(allow) любой трафик по протоколу ICMP(icmp) в любом направлении.(any to any) первым (00001) правилом

ipfw add deny all from 192.168.0.0/24, 10.0.0.0/8 to 192.168.1.0/24
: запретить (deny) любой трафик по любому протоколу (all) в направлении от 192.168.0.0-192.168.0.255 или от 10.0.0.0-10.255.255.255 к подсети 192.168.1.0/24 (192.168.1.0-192.168.1.255). Номер правила в

таком случае берется от последнего использованного +100, за исключением последнего правила по умолчанию (№65535);

ipfw add deny all from 192.168.0.1 to me Запрещает весь трафик от адреса 192.168.0.1 ко всем сетевым интерефейсам устройства, на котором работает конфигурируемый ipfw;

ipfw add allow all from table(1) to any Разрешает весь трафик от адресов в таблице №1 к любым адресам;

ipfw add allow all from table(1) to any out Разрешает весь исходящий (out)

трафик от адресов в таблице №1 к любом адресам;

ipfw add allow all from table(1) to any out via em0 Разрешает весь исходящий (out) трафик от адресов в таблице №1 к любом адресам через интерфейс em0;

ipfw add skipto 1700 ip from table(8) to any Начинает проверять запрос соответствию с правила 1701 (т.е. все правила начиная с данного и до 1700 игнорируются при проверки данного пакета) для ip адресов из таблицы 8;

ipfw add set 31 prob 0.95 allow tcp from me to any out dst-port 80 Разрешает весь исходящий (out) трафик от данного устройства к любому адресу по порту 80 tcp(dst-port 80, tcp) с вероятностью 95% (prob 0.95). Правило добавляется в специальный набор правил №31, см.ниже (ipfw flush);

ipfw table 1 add 192.168.1.2

ipfw table 1 add 192.168.1.128/25 Добавить в таблицу 1 соответственно адрес 192.168.1.2 (маска /32 - по умолчанию) и подсеть 192.168.1.128/25

ipfw table 1 list Показать содержимое таблицы 1;

ipfw delete 00001 удалить ранее созданное правило №1. Описание необязательно - в случае, если под данным номером не одно правило, удаляются все.

ipfw flush удалить все правила, не входящие в набор №31;правило №65535 входит в него по умолчанию;

16.6. См. также

- IPFilter
- Packet Filter
- NPF
- WIpfw
- iptables

16.7. Примечания

[1] *Kuzmich* Настройка FireWall (ipfw) в FreeBSD (рус.). Архивировано из первоисточника 22 марта 2012.

16.8. Ссылки

- Официальное руководство WIPFW (также можно скачать программу) (рус.)
- Официальное руководство (англ.)
- ipfw: порядок прохождения пакетов, сложные случаи
- Учебник по FreeBSD, OpenBSD, NetBSD, DragonFly (BSDA в вопросах и ответах): ipfw
- Установка WIPFW в Windows XP и 2003 x64
- Неофициальный порт wipfw

Глава 17

Iptables

IPTables — утилита командной строки, является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) **netfilter** для ядер Linux, начиная с версии 2.4. Для использования утилиты IPTables требуются привилегии суперпользователя (root).

Иногда под словом IPTables имеется в виду и сам межсетевой экран NETFilter.

17.1. История

Изначально разработка netfilter и iptables шла совместно, поэтому в ранней истории этих проектов есть много общего. Подробности см. в статье про netfilter.

Предшественниками iptables были проекты ipchains (применялась для администрирования фаервола ядра Linux версии 2.2) и ipfwadm (аналогично для ядер Linux версий 2.0). Последний был основан на BSD-утилите ipfw.

iptables сохраняет идеологию, ведущую начало от ipfwadm: функционирование фаервола определяется набором правил, каждое из которых состоит из критерия и действия, применяемого к пакетам, подпадающим под этот критерий. В ipchains появилась концепция *цепочек* — независимых списков правил. Были введены отдельные цепочки для фильтрации входящих (INPUT), исходящих (OUTPUT) и транзитных (FORWARD) пакетов. В продолжении этой идеи, в iptables появились *таблицы* — независимые группы цепочек. Каждая таблица решала свою задачу — цепочки таблицы filter отвечали за фильтрацию, цепочки таблицы nat — за преобразование сетевых адресов (NAT), к задачам таблицы mangle относились прочие модификации заголовков пакетов (например, изменение TTL или TOS). Кроме того, была слегка изменена логика работы цепочек: в ipchains все входящие пакеты, включая транзитные, проходили цепочку INPUT. В iptables через INPUT проходят только пакеты, адресованные самому хосту.

Такое разделение функциональности позволило iptables при обработке отдельных пакетов использовать информацию о соединениях в целом (ранее это было возможно только для NAT). В этом iptables значительно превосходит ipchains, так iptables может отслеживать состояние соединения и перенаправлять, изменять или отфильтровывать пакеты, основываясь не только на данных из их заголовков (источник, получатель) или содержимом пакетов, но и на основании данных о соединении. Такая возможность фаервола называется stateful-фильтрацией, в отличие от реализованной в ipchains примитивной stateless-фильтрации (подробнее о видах фильтрации см. статью о фаерволах). Можно сказать, что iptables анализирует не только передаваемые данные, но и контекст их передачи, в отличие от ipchains, и поэтому может принимать более обоснованные решения о судьбе каждого конкретного пакета. Более подробно о stateful-фильтрации в netfilter/iptables см. Netfilter#Механизм определения состояний.

В будущем, разработчики netfilter планируют заменить iptables на nftables — инструмент нового поколения, пока находящийся в ранней стадии разработки[2].

17.2. Архитектура

17.2.1. Основные понятия

Ключевыми понятиями iptables являются:

- **Правило** — состоит из *критерия*, *действия* и *счетчика*. Если пакет соответствует критерию, к нему применяется действие, и он учитывается счетчиком. Критерия может и не быть — тогда неявно предполагается критерий «все пакеты». Указывать действие тоже не обязательно — в отсутствие действия правило будет работать только как счетчик.
    - **Критерий** — логическое выражение, анализирующее свойства пакета и/или соединения и определяющее, попадает ли данный конкретный пакет под действие текущего правила.

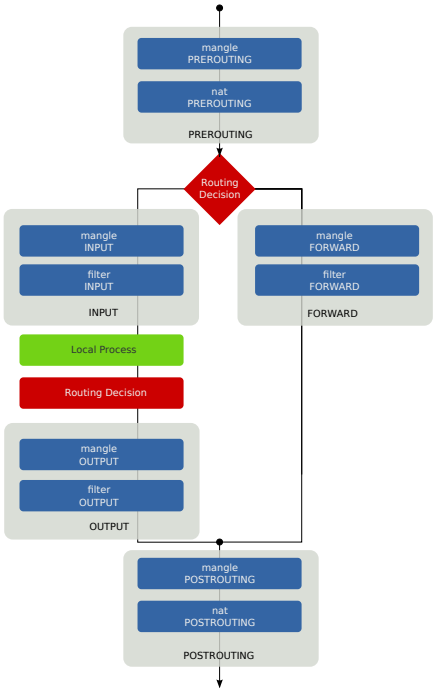


Схема прохождения таблиц

- **Действие** — описание действия, которое нужно проделать с пакетом и/или соединением в том случае, если они попадают под действие этого правила. О действиях более подробно будет рассказано ниже.
- **Счетчик** — компонент правила, обеспечивающий учет количества пакетов, которые попали под критерий данного правила. Также счетчик учитывает суммарный объем таких пакетов в байтах.

- **Цепочка** — упорядоченная последовательность правил. Цепочки можно разделить на *пользовательские* и *базовые*.
  - **Базовая цепочка** — цепочка, создаваемая по умолчанию при инициализации таблицы. Каждый пакет, в зависимости от того, предназначен ли он самому хосту, сгенерирован им или является транзитным, должен пройти положенный ему набор базовых цепочек различных таблиц. Кроме того, базовая цепочка отличается от пользовательской наличием «действия по умолчанию» (default policy). Это действие применяется к тем пакетам, которые не были обработаны другими правилами этой цепочки и вызванных из нее цепочек. Имена базовых цепочек всегда записываются в верхнем регистре (PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING).
  - **Пользовательская цепочка** — цепочка, созданная пользователем. Может использоваться только в пределах своей таблицы. Рекомендуется не использовать для таких цепочек имена в верхнем регистре, чтобы избежать путаницы с базовыми цепочками и встроенными действиями.

- **Таблица** — совокупность *базовых* и *пользовательских* цепочек, объединенных общим функциональным назначением. Имена таблиц (как и модулей критериев) записываются в нижнем регистре, так как в принципе не могут конфликтовать с именами пользовательских цепочек. При вызове команды iptables таблица указывается в формате -t имя_таблицы. При отсутствии явного указания, используется таблица filter.

17.3. Примечания

[1] [ANNOUNCE iptables 1.6.0 release]

[2] Разработчики Netfilter представили замену iptables

17.4. Литература

- *Gregor N. Purdy.* Linux iptables. Pocket Reference. — O'Reilly, 2004. — С. 97. — ISBN 0-596-00569-5.

17.5. Ссылки

- Сайт проекта Netfilter
- Man page of iptables (англ.)
- Руководство по iptables (Iptables Tutorial 1.1.19)* (рус.)

Глава 18

Jetico Personal Firewall

Jetico Personal Firewall — межсетевой экран разработанный фирмой Jetico, занимающейся разработкой криптографического программного обеспечения.

18.1. Возможности

Так же как и большинство программных фаерволлов, Jetico Personal Firewall позволяет применять специфические правила для сетевой активности. Также Jetico Personal Firewall производит мониторинг процессов для предотвращения инъекций кода, производит валидацию сетевых пакетов и параметров, ведёт лог сетевой активности.

18.2. История версий

18.2.1. Версия 1.0

Версия 1 поддерживает операционные системы Windows 98, Me, NT, 2000 и XP.

Версия 1.0.1.47 была представлена общественности 30 декабря 2004 года, после нескольких бета-версий и релиз-кандидатов. По состоянию на 1 августа 2006 года, разработка Jetico Personal Firewall версии 1 была остановлена.[1]

Список изменений в ревизиях 1-й версии можно найти здесь. На данный момент 1-я версия продукта доступна для бесплатного использования.

18.2.2. Версия 2.0

Jetico Personal Firewall версии 2 поддерживает 32-х и 64-х битные версии операционных систем Windows 2000, 2003 Server, XP, Vista, Windows 7, Windows 8.

Версия 2.0.0.30 была представлена общественности 23 апреля 2007 года.

Версия 2 работает как привилегированная служба в Windows, что позволяет ей функционировать ещё до того как пользователь залогинится. Также это даёт возможноть быстрого переключения между пользователями и терминальными службами. Версия 2 интергрируется в центр безопасности Windows XP Service Pack 2.[2]

Список изменений для версии 2 можно посмотреть здесь.

18.3. Поддержка

Пользователи могут получить поддержку у представителей фирмы Jetico и других пользователей на официальном форуме поддержки Jetico Personal Firewall Support forum.

Другие способы связи представлены здесь.

18.4. Примечания

[1] Jetico - Jetico Personal Firewall

[2] Jetico - Jetico Personal Firewall

18.5. Ссылки

- Официальный сайт Jetico Personal Firewall

Глава 19

Kaspersky Internet Security

Kaspersky Internet Security (KIS) — линейка программных продуктов, разработанная компанией «Лаборатория Касперского» на базе линейки продуктов Антивирус Касперского, для комплексной защиты домашних персональных компьютеров в реальном времени от известных и новых современных угроз.

19.1. Функционал программы

В продукте реализованы следующие основные функции:

- гибридная антивирусная защита в реальном времени, которая сочетает в себе возможности:
  - традиционных сигнатурных технологий;
  - современных технологий (проактивные эвристические методы);
  - облачных технологий;
- защита от эксплойтов для предотвращения использования уязвимостей на компьютере;
- функция отката, позволяющая устранить последствия деятельности вредоносных программ;
- средства от интернет-мошенничества (в частности, фишинга и кейлоггеров) для повышения степени защиты личных данных и другой ценной информации;
- защита данных при выполнении финансовых операций в интернете:
  - пользовании системами онлайн-банкинга;
  - пользовании платежными системами (в частности, PayPal, Яндекс.Деньги и другие);
  - совершении покупок в интернете;
- защита от сетевых хакерских атак;
- **Контроль изменений (сообщает** о готовящихся изменениях параметров браузера, в том числе вызванных установкой рекламных программ, панелей инструментов);
- **Защита от сбора данных** (запрещает сайтам отслеживать сценарии пользования интернетом и собирать личные данные);
- **Контроль интернет-трафика (**помогает оптимизировать расходы при подключении к интернету через Wi-Fi, 3G и 4G);
- **Защита от программ-шифровальщиков;**
- **Проверка безопасности публичных сетей Wi-Fi** (помогает защитить от кражи данных через незащищенные сети);
- **Защита от несанкционированного подключения к веб-камере;**
- **Поиск уязвимостей в программах;**
- **Режим Безопасных программ** (разрешает запуск только доверенных приложений и ограничивает работу всех подозрительных программ);
- обеспечение актуальной информацией о репутации программ и веб-сайтов;
- блокирование нежелательного контента (в частности, рекламных баннеров и спам-рассылок);
- управление доступом детей к веб-сайтам и программам, а также контроль их общения в социальных сетях, ICQ и так далее;
- средства для восстановления системы в случае заражения на основе Live CD.

19.2. Состав компонентов защиты

Защита компьютера в реальном времени обеспечивается следующими компонентами защиты[3]:

1. Файловый Антивирус
2. Контроль программ
3. Защита от сетевых атак

4. IM-антивирус
5. Почтовый антивирус
6. Доступ к веб-камере
7. Защита от сбора данных
8. Веб-антивирус
9. Сетевой экран
10. Мониторинг активности
11. Контроль изменений в операционной системе
12. Анти-спам
13. Анти-баннер
14. Безопасные платежи
15. Виртуальная клавиатура
16. Безопасный ввод данных
17. Родительский контроль
18. Защита веб-камеры
19. Проверка безопасности Wi-Fi
20. Мониторинг сети

19.3. Системные требования

19.3.1. Для ОС Windows

- Windows XP (Home Edition, Professional Service, x64 Edition) Service Pack 2 и выше:
  - Процессор 800 МГц и выше
  - 512 Мб свободной оперативной памяти
- Windows Vista, Windows 7, Windows 8 (поддерживается с версии 13.0.1.4190):
- Windows 8.1 поддерживается с версии 14.0.0.4651
  - Процессор 1 ГГц и выше
  - 1 Гб свободной оперативной памяти (x32) или 2 Гб свободной оперативной памяти (x64)
  - Windows 10
  -

Общие требования для всех операционных систем:

- Около 480 Мб свободного пространства на жёстком диске (в зависимости от размера антивирусных баз)
- CD-ROM для установки программы с диска
- Компьютерная мышь
- Подключение к интернету для активации продукта и получения регулярных обновлений
- Internet Explorer 8.0 или выше
- Windows Installer 3.0 или выше
- Microsoft.NET Framework 4 и выше

Аппаратные требования для нетбуков:

- Процессор: Intel Atom 1,6 ГГц
- Видеокарта: Intel GMA950
- Экран: 10,1”
- Операционная система: Microsoft Windows XP Home Edition

19.3.2. Для Mac

- Mac OS X 10.7 — 10.10
- 1 Гб оперативной памяти
- Около 500 Мб свободного пространства на жестком диске (в зависимости от размера антивирусных баз)
- Интернет-соединение для активации продукта и получения регулярных обновлений

19.3.3. Для Android

- Android 2.3 – 4.4
- Минимальное разрешение экрана: 320 x 480

19.4. Статус поддержки программы

19.5. Награды

- В апреле 2009 Kaspersky Internet Security 2009 получил премию «Золотой Компьютер» журнала ComputerBild. Решение стало победителем в номинации Soft и обладателем главного приза как продукт, получивший абсолютное число голосов в свою поддержку.
- В апреле 2009 по итогам сравнительного исследования, проведённого журналом «Мир ПК», Kaspersky Internet Security 2009 получил награду «Выбор редакции»

- В апреле 2009 в рамках сравнительного тестирования, проведённого независимой китайской тестовой лабораторией PC Security Labs, продукт Kaspersky Internet Secuirty 2009 набрал 99,50 баллов из 100 возможных и получил максимальную оценку в пять звезд.

- В марте 2009 крупнейший датский новостной портал по IT-тематике Tweakup.dk протестировал Kaspersky Internet Security 2009 и присвоил решению рейтинг в 9,5 пунктов из 10 возможных.[4]

- 9 августа 2007 года в прессе появилась информация о том, что антивирус Kaspersky Internet Security шестой версии «Лаборатории Касперского» вошёл в десятку компьютерных программ, пользующихся наибольшим спросом в крупнейшем по обороту интернет-магазине мира Amazon.com.[5]

- По результатами Proactive Security Challenge Kaspersky Internet Security 2012 12.0.0.374 занял седьмое место с результатом 93 % и оценкой Excellent (Отлично). Рекомендован к применению.[6]

- Platinum Self-Protection Award (сентябрь 2010, февраль 2011) от Anti-Malware.ru.[7][8]

- Gold Personal IDS/IPS Award (июнь 2011)[9]

- Gold Parental Control Award (декабрь 2012 г.) от Anti-Malware.ru[10]

- AV-Comparatives: Тестирование защиты от фишинга: Август 2013; Высший уровень защиты.

19.6. «Пасхальное яйцо»

Если в титрах, идущих в окне «О программе» версий, начиная с 7.0[11], щёлкнуть мышью по имени Евгения Касперского, появляется фото, где он показывает «Превед!». Стойка Евгения Касперского в точности повторяет стойку медведя из русской редакции картины «Bear Surprise» Джона Лури.

19.7. См. также

- Антивирус Касперского
- Kaspersky CRYSTAL
- Kaspersky Password Manager
- Kaspersky Mobile Security

19.8. Примечания

[1] Обзор KIS 6.0 (рус.). Обзор Kaspersky Internet Security 6.0 - нового продукта Лаборатории Касперского. Проверено 16 октября 2006. Архивировано из первоисточника 13 мая 2013.

[2] Статус поддержки программ для защиты персональных компьютеров. Официальный сайт технической поддержки. Проверено 4 сентября 2012. Архивировано из первоисточника 18 октября 2012.

[3] Выдержка из справки антивируса

[4] Награды

[5] «Касперский» в десятке. Антивирус компании занимает верхние строчки продаж Amazon

[6] Results and comments — www.matousec.com

[7] Тест самозащиты антивирусов, сравнение антивирусов (сентябрь 2010) — Тесты и сравнения антивирусов — Anti-Malware.ru

[8] Тест самозащиты антивирусов на платформе Windows 7 x64 (январь 2011) — Тесты и сравнения антивирусов — Anti-Malware.ru

[9] *Михаил Картавенко.* Тест персональных IDS/IPS на защиту от атак на уязвимые приложения (июнь 2012) - Тесты и сравнения антивирусов. *Anti-Malware.ru* (1 июня 2012). Проверено 10 июня 2012. Архивировано из первоисточника 10 июня 2012.

[10] *Александр Панасенко.* Тест, сравнение интернет-фильтров для детей - родительских контролей (декабрь 2012) - Тесты и сравнения антивирусов. *Anti-Malware.ru* (20 декабря 2012). Проверено 21 января 2013. Архивировано из первоисточника 21 января 2013.

[11] Для отображения титров нужно нажать на название продукта (в версии 7.0 при этом надо удерживать нажатыми правую кнопку мыши и клавишу Control, в версиях, начиная с 2009 (8.0) достаточно простого щелчка)

19.9. Литература

- *Сергей Трошин* Есть смысл подумать // UP Special : журнал. — 2010. — Октябрь (№ 10). — С. 88—89. — ISSN 1729-438X.

- *Акустик* Опережая календарь // UPgrade : журнал. — 2011. — 29 августа (№ 33). — С. 36—37. — ISSN 1680-4694.

19.10. Ссылки

- Информация о Kaspersky Internet Security на сайте Лаборатории Касперского

- Список программ, несовместимых с Kaspersky Internet Security 2011
- Обзор Kaspersky Internet Security 2010 на 3DNews
- Обзор Kaspersky Internet Security 2013 на Anti-Malware.ru
- Обзор и тестирование KIS 2011 на foxnetwork.ru
- *Андрей Болтушкин.* Обзор программы Kaspersky Internet Security 2011. SoftSalad.ru (18 апреля 2011). Архивировано из первоисточника 25 февраля 2012.

Глава 20

Kerio Control

Kerio Control (ранее назывался Kerio WinRoute Firewall и WinRoute Pro) — это программный межсетевой экран, разработанный компаниями Kerio Technologies и Tiny Software. Основными функциями программы являются: организация безопасного пользовательского доступа в Интернет, надежная сетевая защита ЛВС, экономия трафика и рабочего времени сотрудников за счёт ограничения нецелевого доступа к различным категориям веб-контента.

20.1. Особенности программы

- Многоязычный интерфейс (16 языков, включая русский)
- Встроенный прокси-сервер
- Интегрированный антивирус от Sophos
- Возможность подключения дополнительных антивирусных модулей
- Контроль пропускной полосы канала
- Балансировка нагрузки на каналы
- Реализован собственный VPN
- Мониторинг и протоколирование пользовательской активности в Интернет
- Интеграция с Active Directory

20.2. Версии

20.3. Ссылки

- Официальный сайт разработчика программы
- Официальный сайт для пользователей СНГ
- Центр Поддержки
- Официальный форум программы

Глава 21

L7-filter

l7-filter — программный пакет, представляющий собой классификатор для подсистемы Netfilter в ОС Linux, который может распределять по категориям IP-пакеты, базируясь на данных прикладного уровня. Основная цель этого инструмента заключается в том, чтобы сделать возможным выявление трафика файлообменных сетей (также p2p), клиенты которых используют непредсказуемое число портов.

Существуют две версии этого программного продукта. Первая реализована в виде модуля для ядра Linux 2.4 и 2.6. Вторая экспериментальная версия была выпущена в декабре 2006 года в качестве userspace-приложения, и для классификации опирается на пользовательское пространство библиотек netfilter.

Обе версии l7-filter используют регулярные выражения (хотя в версиях пользовательского пространства и модулей ядра используются различные библиотеки регулярных выражений) для определения сетевого протокола. Этот метод, который используется в сочетании с системой QoS ОС Linux, позволяет применение более специфического, чем порт-независимого формирования трафика.

Все версии l7-filter были опубликованы в соответствии с GNU General Public License.

21.1. Ссылки

- **l7-filter.sourceforge.net** — официальный сайт L7-filter
- Wiki: methods of identifying application layer network protocols (Проверено 13 января 2010)

Глава 22

Little Snitch

Little Snitch - межсетевой экран для Mac OS X. Производится и поддерживается австрийской компанией Objective Development Software GmbH.

Если приложение или процесс пытается установить исходящее соединение в интернет, Little Snitch предотвращает попытку. Пользователю выводится диалоговое окно, позволяющее разрешить или запретить соединение однократно или постоянно. Возможно создать ограничивающие правила на основе определённого порта, домена или протокола соединения. Режим сетевого монитора позволяет отслеживать проходящий трафик в реальном времени с отображением доменных имён и направления трафика.

Программа получила 4,5 звезды из 5 издания Macworld в 2008 году.[1]

22.1. Примечания

[1] Little Snitch 2.0.3 Review | Macworld

22.2. Ссылки

- Русскоязычный сайт Little Snitch
- Инструкция по установке и настройке Little Snitch

Глава 23

Microsoft Forefront Threat Management Gateway

Microsoft Forefront Threat Management Gateway (Forefront TMG; ранее известный как Microsoft Internet Security and Acceleration Server (ISA Server)) — прокси-сервер для защиты сети от атак извне, а также контроля интернет-трафика, который «позволяет сотрудникам компании безопасно и эффективно пользоваться ресурсами Интернета, не беспокоясь о вредоносных программах и других угрозах»[1].

9 сентября 2012 Microsoft объявила о прекращении дальнейшего развития Forefront TMG. Основная поддержка будет прекращена после 14 апреля 2015 года, а расширенная поддержка закончится 14 апреля 2020 года. Продукт не будет доступен для приобретения после 1 декабря 2012 года[2].

23.1. Описание

Продукт пришёл на смену Microsoft Internet Security and Acceleration Server (ISA Server), ещё ранее прокси-серверу Microsoft Proxy Server от Microsoft.

Позволяет организовать защиту локальной сети от вмешательств из сети Интернет и безопасно публиковать различные виды серверов, дает возможность распределять доступ пользователей локальной сети к ресурсам Интернет. Оснащен средствами для анализа посещаемых ресурсов, учёта трафика, а также защиты против атак из сети Интернет. Имеет различные виды аутентификации и авторизации, в том числе поддерживает аутентификацию Active Directory. Поддерживает как рабочие группы, так и домены Windows NT. Имеет множество плагинов для отслеживания исходящего и входящего трафика.

23.2. Версии

23.2.1. Microsoft Proxy Server

В 1996 году война браузеров между Microsoft Internet Explorer и Netscape Navigator была в самом разгаре и Microsoft искала возможности для улучшения позиций своего браузера. В это время, компания Netscape начала продажи web прокси сервера Netscape Proxy Server, позволявшего экономить время загрузки и расходы на дорогой интернет трафик путём кэширования изображений и веб страниц локальным сервером. Прямым ответом на это, в октябре 1996 года был выпущен Microsoft Proxy Server v1.0 (кодовое имя *Catapult*) рассчитанный на работу с Windows NT 4.0[3].

Microsoft Proxy Server v2.0 был выпущен в декабре 1997 года и принёс такие возможности как создание массива прокси серверов, функцию обратного прокси (англ. *Reverse proxy*) и обратного хостинга (reverse hosting, сервер отвечает на входящие web-запросы за серверы, стоящие позади него).

23.2.2. ISA Server 2000

18 марта 2001 года был выпущен Microsoft Internet Security and Acceleration Server 2000[4]. Новая версия принесла такие возможности, как обнаружение вторжений, поддержка Active Directory и виртуальных частных сетей (VPN), SecureNAT, разделение полосы пропускания и другие возможности. ISA Server 2000 был представлен в *Standard* и *Enterprise* редакциях. Такие технологии, как High-Availability Clustering не были включены в Standard Edition. ISA Server 2000 требовал для работы Windows 2000 (любой редакции, кроме Professional), а также работал на Windows Server 2003.

23.2.3. ISA Server 2004

Microsoft Internet Security and Acceleration Server 2004 выпущен 8 сентября 2004 года[5].

23.2.4. ISA Server 2006

17 октября 2006 года был выпущен Microsoft Internet Security and Acceleration Server 2006[6]. Это обновлённая версия ISA Server 2004 сохранила все возможности Server 2004 за исключением Message Screener.

23.2.5. Microsoft Forefront Threat Management Gateway 2010

Microsoft Forefront Threat Management Gateway 2010 (Forefront TMG 2010) выпущен 17 ноября 2009[7]. Эта версия основана на ISA Server 2006 и обеспечивает улучшенную защиту веб трафика, родную поддержку 64 битных систем, поддержку Windows Server 2008 и Windows Server 2008 R2 и встроенную защиту от вредоносных программ.

23.2.6. Прекращение дальнейшего развития

9 сентября 2012 Microsoft объявила о прекращении дальнейшего развития Forefront TMG. Основная поддержка будет прекращена после 14 апреля 2015 года, а расширенная поддержка закончится 14 апреля 2020 года. Продукт не будет доступен для приобретения после 1 декабря 2012 года[2]. На сегодняшний день доступен только в составе аппаратных решений OEM партнёров Microsoft.

23.3. Примечания

[1] Скачать Forefront Threat Management Gateway (TMG) 2010

[2] Important Changes to Forefront Product Roadmaps. *Server & Cloud Blog*. Microsoft corporation (12 September 2012). Архивировано из первоисточника 18 октября 2012.

[3] Microsoft Ships Proxy Server 1.0. Проверено 13 апреля 2012. Архивировано из первоисточника 3 июня 2012.

[4] Microsoft Support Lifecycle ISA 2000. Проверено 25 июня 2012. Архивировано из первоисточника 27 июня 2012.

[5] Microsoft Support Lifecycle ISA 2004. Проверено 25 июня 2012. Архивировано из первоисточника 27 июня 2012.

[6] Microsoft Support Lifecycle ISA 2006. Проверено 25 июня 2012. Архивировано из первоисточника 27 июня 2012.

[7] Forefront Threat Management Gateway 2010 Release. *Forefront TMG (ISA Server) team blog*. Microsoft corporation (17 November 2009). — «It is our pleasure to announce that Forefront Threat Management Gateway (TMG) 2010 was released to manufacturing yesterday (Nov 16th, 2009) [~snip~]» Проверено 26 марта 2010. Архивировано из первоисточника 17 февраля 2012.

23.4. Литература

- *Майкл Ноэл.* Microsoft ISA Server 2006. Полное руководство = Microsoft ISA Server 2006 Unleashed. — М.: «Вильямс», 2008. — С. 624. — ISBN 978-5-8459-1486-6.

23.5. Ссылки

- Microsoft Forefront Threat Management Gateway
- Microsoft ISA Server и Forefront TMG на русском языке
- Обзор вариантов замены Forefront TMG (включая российские аналоги)

Глава 24

Netfilter

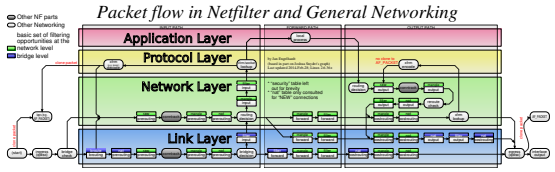
Netfilter — межсетевой экран (брандмауэр), встроен в ядро Linux с версии 2.4.

24.1. Название

iptables — название пользовательской утилиты (запускаемой из командной строки) предназначенной для управления системой netfilter. С её помощью администраторы создают и изменяют правила, управляющие фильтрацией и перенаправлением пакетов. Для работы с семейством протоколов IPv6 существует отдельная версия утилиты iptables — ip6tables.

Некоторые авторы под словом netfilter имеют в виду только те элементы межсетевого экрана, которые непосредственно являются частью стека протоколов ядра, а всё прочее (систему таблиц и цепочек) называют iptables[1]. Из-за не совсем ясной терминологии, иногда весь проект (внутриядерный межсетевой экран вместе с пользовательской утилитой) просто именуется **netfilter/iptables**.

24.2. История



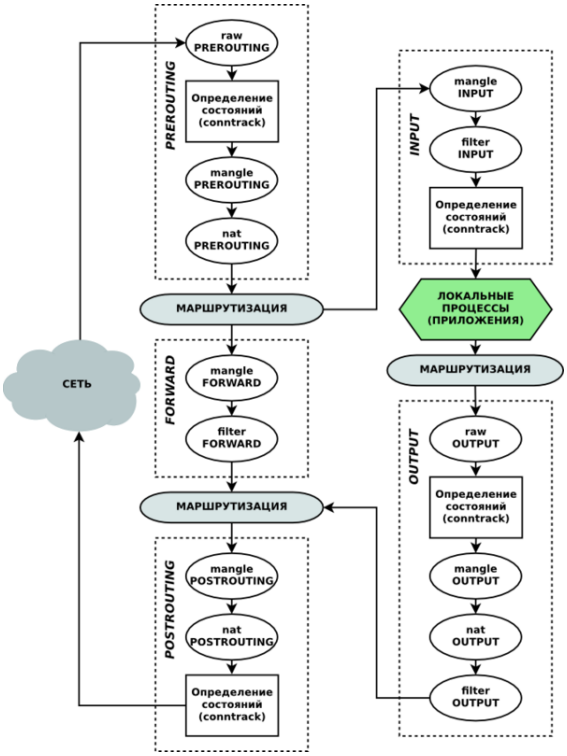
Flow of network packets through Netfilter

Проект netfilter/iptables был основан в 1998. Автором является Расти Расселл (en:Rusty Russell); он же автор проекта-предшественника ipchains. По мере развития проекта, в 1999 г. образовалась команда Netfilter Core Team (сокращено coreteam). Разработанный межсетевой экран получил официальное название netfilter. В марте 2000 г. был включен в ядро Linux 2.3. В августе 2003 руководителем coreteam стал Харальд Вельте (Harald Welte). В 2004 г. Вельте начал и выиграл судебный процесс против компании Sitecom GmbH, которая использовала netfilter в своей продукции, но отказывалась следовать лицензии GNU GPL[2].

До появления iptables, для обеспечения возможностей межсетевого экрана в Linux использовались проекты ipchains в Linux 2.2 и ipfwadm в Linux 2.0, в свою очередь основанный на ipfw из системы BSD. Проекты ipchains и ipfwadm изменяли работу стека протоколов ядра Linux, поскольку до появления netfilter в архитектуре ядра не существовало возможностей для подключения дополнительных модулей управления пакетами. iptables сохранил основную идею ipfwadm — список правил, состоящих из критериев и действия, которое выполняется если пакет соответствует критериям. В ipchains была представлена новая концепция — возможность создавать новые цепочки правил и переход пакетов между цепочками, а в iptables концепция была расширена до четырёх таблиц, разграничивающих цепочки правил по задачам: фильтрация, NAT, и модификация пакетов. Также iptables расширил возможности Linux в области определения состояний, позволяя создавать межсетевые экраны, работающие на сеансовом уровне.

24.3. Архитектура

В системе netfilter пакеты пропускаются через **цепочки**. Цепочка является упорядоченным списком **правил**, а каждое правило может содержать **критерии** и **действие** или **переход**. Когда пакет проходит через цепочку, система netfilter по очереди проверяет, соответствует ли пакет всем критериям очередного правила, и если так, то выполняет действие (если критериев в правиле нет, то действие выполняется для всех пакетов, проходящих через правило). Вариантов возможных критериев очень много. Например, пакет соответствует критерию --source 192.168.1.1 если в заголовке пакета указано, что отправитель — 192.168.1.1. Самый простой тип перехода, --jump, просто пересылает пакет в начало другой цепочки. Также при помощи --jump можно указать действие. Стандартные действия доступные во всех цепочках — *ACCEPT* (пропустить), *DROP* (удалить), *QUEUE*



Путь проверки пакета в системе netfilter

(передать на анализ внешней программе), и *RETURN* (вернуть на анализ в предыдущую цепочку). Например, команды

iptables -A INPUT --source 192.168.1.1 --jump ACCEPT iptables -A INPUT --jump other_chain

означают «добавить к концу цепочки *INPUT* следующие правила: пропустить пакеты из 192.168.1.1, а всё, что останется — отправить на анализ в цепочку *other_chain*».

24.3.1. Цепочки

Существует 5 типов стандартных цепочек, встроенных в систему:

- **PREROUTING** — для изначальной обработки входящих пакетов.
- **INPUT** — для входящих пакетов, адресованных непосредственно локальному процессу (клиенту или серверу).
- **FORWARD** — для входящих пакетов, перенаправленных на выход (заметьте, что перенаправляемые пакеты проходят сначала цепь *PREROUTING*, затем *FORWARD* и *POSTROUTING*).
- **OUTPUT** — для пакетов, генерируемых локальными процессами.
- **POSTROUTING** — для окончательной обработки исходящих пакетов.

Также можно создавать и уничтожать собственные цепочки при помощи утилиты iptables.

24.3.2. Таблицы

Цепочки организованны в 4 таблицы:

- **raw** — просматривается до передачи пакета системе определения состояний. Используется редко, например для маркировки пакетов, которые НЕ должны обрабатываться системой определения состояний. Для этого в правиле указывается действие *NOTRACK*. Содержит цепочки *PREROUTING* и *OUTPUT*.
- **mangle** — содержит правила модификации (обычно заголовка) IP-пакетов. Среди прочего, поддерживает действия *TTL (Time to live)*, *TOS (Type of Service)*, и *MARK* (для изменения полей TTL и TOS, и для изменения маркеров пакета). Редко необходима и может быть опасна. Содержит все пять стандартных цепочек.
- **nat** — просматривает только пакеты, создающие новое соединение (согласно системе определения состояний). Поддерживает действия *DNAT*, *SNAT*, *MASQUERADE*, *REDIRECT*. Содержит цепочки *PREROUTING*, *OUTPUT*, и *POSTROUTING*. Для версий ядра >2.6.35 в таблицу **nat** также добавлена цепочка *INPUT*[3][4].
- **filter** — основная таблица, используется по умолчанию если название таблицы не указано. Содержит цепочки *INPUT*, *FORWARD*, и *OUTPUT*.

Цепочки с одинаковым названием, но в разных таблицах — совершенно независимые объекты. Например, *raw PREROUTING* и *mangle PREROUTING* обычно содержат разный набор правил; пакеты сначала проходят через цепочку *raw PREROUTING*, а потом через *mangle PREROUTING*.

24.3.3. Механизм определения состояний

Механизм определения состояний (state machine, connection tracking) — система трассировки соединений, важная часть netfilter, при помощи которой реализуется межсетевой экран на сеансовом уровне (stateful firewall). Система позволяет определить, к какому соединению или сеансу принадлежит пакет. Механизм определения состояний анализирует все пакеты кроме тех, которые были помечены *NOTRACK* в таблице *raw*.

В системе netfilter каждый пакет, проходящий через механизм определения состояний, может иметь одно из четырёх возможных состояний:

- **NEW** — пакет открывает новый сеанс. Классический пример — пакет TCP с флагом SYN.
- **ESTABLISHED** — пакет является частью уже существующего сеанса.
- **RELATED** — пакет открывает новый сеанс, связанный с уже открытым сеансом. Например, во время сеанса пассивного FTP, клиент подсоединяется к порту 21 сервера, сервер сообщает клиенту номер второго, случайно выбранного порта, после чего клиент подсоединяется ко второму порту для передачи файлов. В этом случае второй сеанс (передача файлов по второму порту) связан с уже существующим сеансом (изначальное подсоединение к порту 21).
- **INVALID** — все прочие пакеты.

Эта классификация пакетов во многих случаях отличается от официального описания сетевых протоколов. Например, согласно netfilter, TCP пакет ACK отвечающий на SYN — часть существующего сеанса, а по определению TCP такой пакет — всего лишь элемент открытия сеанса.

Определить сеансы некоторых протоколов очень просто; например, признак сеанса UDP — клиент с порта X посылает серверу на порт Y (или наоборот) пакеты не реже чем раз в 30 секунд. У других протоколов (FTP, SIP, H.323 и т. д.) сеанс определить сложнее, и netfilter должен анализировать содержимое пакетов чтобы правильно определить их состояние.

Просмотреть атрибуты активных подключений можно в псевдо-файле /proc/net/nf_conntrack (или /proc/net/ip_conntrack). Для каждого подключения указывается информация следующего вида:

tcp 6 117 SYN_SENT src=192.168.1.6 dst=192.168.1.9 sport=32775 dport=22 [UNREPLIED] src=192.168.1.9 dst=192.168.1.6 sport=22 dport=32775 [ASSURED] use=2

Утилита conntrack позволяет управлять механизмом определения состояний.

24.4. См. также

nftables (англ.) — проект, который призван заменить существующую связку {ip,ip6,arp,eb}tables.

24.5. Примечания

[1] *Coulson, David* Mastering IPTables (англ.). www.linuxformat.co.uk (4 апреля 2001).

[2] Urteil Harald Welte gegen Sitecom Deutschland GmbH (нем.). Мюнхенский суд (19 мая 2004). Архивировано из первоисточника 24 февраля 2012.

[3] iptables: built-in INPUT chain in nat table? - Server Fault

[4] kernel/git/torvalds/linux.git - Linux kernel source tree

24.6. Ссылки

- Сайт проекта
- Iptables Tutorial в русском переводе
- Статья о механизме определения состояний в netfilter

24.6.1. Администрирование netfilter

- Firewall Builder
- dwall All-purpose firewall generator
- Firestarter Визуальный редактор
- NetfilterOne A free graphical tool for managing Netfilter's security policy (This software is no longer available directly from Solsoft)
- KMyFirewall Графический интерфейс (GUI) на основе KDE/Qt
- GIPT — C++/Qt API
- firehol — инструмент, позволяющий компактно описывать межсетевые экраны

Глава 25

Norton 360

Norton 360 — пакет безопасности разработанный компанией Symantec. Пакет включает в себя файрвол, защиту от фишинга, антивирус. Также в пакет входит набор утилит по резервному копированию системы и по её настройке и оптимизации (чистка временных файлов, дефрагментация). Norton 360 выпускается для 32-битной Windows XP и для 32- и 64-битной Windows Vista[1][2]. В версиях 3.5.2.** и выше появилась полная поддержка Windows 7.

25.1. История версий

25.1.1. Версия 1.0

Первая версия была выпущена 26 февраля 2007 года. Это был первый продукт Symantec использовавший SONAR для обнаружения вирусов. Программа следила за приложениями и принимала необходимые меры.[3] Norton 360 позволял пользователю очистить временные файлы и историю браузера. Также программа предоставляла пользователям возможность резервного копирования на сервер в интернете, на жесткий диск, на CD и на DVD. Системные требования программы для Windows XP составляли 300 МГц процессора, 256 мегабайт оперативной памяти и 300 Мб на жестком диске. Для Windows Vista — процессор на 800 МГц, 512 Мб ОЗУ и 300 Мб дискового пространства.

Norton 360 требовал меньше системных ресурсов чем Norton Internet Security 2007 и обладал защитой от фишинга. CNET отметил отсутствие защиты от фишинга для всех браузеров, кроме IE. Также было отмечено отсутствие беспроводных сетевых инструментов, таких как уведомление пользователей, когда кто-то незваный присоединяется к сети при помощи шифрования беспроводных сигналов. PC Magazine критиковали фильтрацию спама в версии 1.0: они установили, что Norton 360 заблокировал только половину от спам-почты и по ошибке заблокировал 5% обычной почты.[4]

25.1.2. Версия 2.0

Версия 2.0 была выпущена 3 марта 2008. В новой версии резервное копирование можно было осуществлять также на Blu-Ray и HD DVD-диски. При резервном копировании в Интернет пользователь мог осуществлять контроль трафика который использует программа[5]. Была добавлена защита от фишинга для браузера Firefox. Добавилось приложение Norton Idnetity Safe сохраняющее параметры входа на сайт. Системные требования остались такими же ка у версии 1.0. PC Magazine назвал спам фильтр слабым: он заблокировал 25 % нормальной почты[6]. CNET сообщил о возникновении проблем при установке программы на некоторые машины[7].

25.1.3. Версия 3.0

Версия 3.0 была выпущена 4 марта 2009 года[8]. Эта версия использует тот же код что и Norton Internet Security 2009. Для более ранних версий в Symantec писался отдельный код[9].

В версии 3.0 появился Norton Safe Web, предлагавшийся ранее как отдельная услуга. Safe Web интегрируется в IE и Firefox и запрещает доступ к вредноносным и мошенническим сайтам.(Примечание)-"Также safe web стал интегрироваться и в браузер Google Chrome,но это уже в более поздних версиях программы Нортон−360.Например в версии Нортон−360 6.0.Версия Нортон−360 6.0-это последняя версия,которая вышла уже в 2012 году.В данной статье сказано только о более ранних версиях антивирусной программы Нортон−360.Последняя версия Нортон−360 6.0 от 2012 года значительно улучшена и доработана корпорацией symantec"... Эта панель также включала в себя поиск от ask.com. Панель инструментов от ask.com имеет отдельный код который был признан некоторыми антивирусами программой шпионом[10]. Из-за критики компании SYMANTEC сообщил что не будет использовать панель ask.com в будущих версиях программы[10][11][12].

В третьей версии программы появилась возможность резервного копирования на флеш-диск. Файл, хранящийся на флеш-диске, может быть скопирован на

другой компьютер без использования Norton 360. Norton 360 не сохраняет предыдущие версии файлов и пропускает открытые файлы. Также, в этой версии появился менеджер запуска приложений, что позволяет пользователю контролировать приложения у него на компьютере и оценить воздействие программы на момент запуска.[13].

PC Magazine назвал спам-фильтр слабым: он принял половину обычной почты за спам.

25.2. Примечания

[1] Norton is ready for Windows 7. Symantec. Проверено 15 мая 2009. Архивировано из первоисточника 26 февраля 2012.

[2] Windows 7 Beta Compatibility. Symantec. Проверено 15 мая 2009. Архивировано из первоисточника 26 февраля 2012.

[3] *Robert McMillan.* Symantec unveils SONAR to find zero-day attacks. Infoworld (17 января 2007). Проверено 4 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[4] *Robert Vamosi.* Norton 360. PC Magazine (26 февраля 2007). Проверено 20 мая 2009. Архивировано из первоисточника 26 февраля 2012.

[5] Norton 360 version 2.0 Tuned Up Tuneup. PC Magazine. Проверено 27 февраля 2009. Архивировано из первоисточника 26 февраля 2012.

[6] Norton 360 version 2.0 Updated Add-Ons. *Neil J. Rubenking*. PC Magazine (March 13, 2008). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[7] Norton 360 2.0. *Robert Vamosi.* CBS Interactive Inc (March 3, 2008). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[8] Symantec Releases Norton 360 version 3.0. *ChannelTimes Staff*. ITNation India Pvt. Ltd (April 1, 2009). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[9] Symantec Sends Slimmed-Down Norton 360 to Beta. *Neil J. Rubenking*. PC Magazine (December 25, 2008). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[10] Critics: Ask Jeeves Silently Serves Software. *Jay Lyman*. ECT News Network, Inc (September 13, 2005). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[11] Norton 360 Version 3.0 Blocking Bad Web Sites. *Neil J. Rubenking*. PC Magazine (March 13, 2009). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[12] Safe Search update. *Rowan Trollope*. Symantec Corporation (March 17, 2009). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

[13] Norton 360 Version 3.0 PC Tuneup. *Neil J. Rubenking*. PC Magazine (13 марта 2009). Проверено 5 апреля 2009. Архивировано из первоисточника 26 февраля 2012.

25.3. Ссылки

- Norton 360
- Магазин Norton
- *Ростислав Панчук.* Системные утилиты 2008 - новые продукты, новые возможности // Домашний ПК. — 2008. — № 9. — С. 80-83.

Глава 26

Norton Internet Security

Norton Internet Security (сокращенно NIS) — пакет безопасности, разработанный компанией Symantec. Включает в себя антивирус, брандмауэр, сканер электронной почты, фильтр спама, защиту от фишинга[1]. Дополнительные функции, такие как, например,Родительский контроль, имеются в расширениях, разработанных компанией Symantec[2]. Доля Norton Internet Security составляла 61% всего рынка аналогичного ПО в США в 2007 году.

Существуют версии для Windows и MAC.

26.1. История версий для WINDOWS

В 1990 году компания Symantec приобрела компанию Питера Нортона Peter Norton Computing[3]. Компания Peter Norton Computing занималась разработкой разнообразных приложений для DOS, в том числе и антивируса. Symantec продолжила развитие приобретенных технологий и начала выпускать программы с названием Norton и пометкой «от Symantec».

Пользователи версий 2006, 2007 и 2008 могут перейти на версию 2009, не покупая новой лицензии. Количество дней, оставшихся до окончания старой лицензии, не изменяется[4].

26.1.1. Версия 2000 (1.0)

Версия 2000 официально появилась 10 января 2000 года. Файрвол Norton Internet Security был основан на межсетевом экране AtGuard, который был первоначально разработан WRQ Inc. и приобретен компанией Symantec

26.1.2. Версия 2006 (13.0)

Версия 2006 официально появилась 26 сентября 2005 года.

26.1.3. Версия 2007 (14.0)

Версия 2007 официально появилась 12 сентября 2006 года.

26.1.4. Версия 2008 (15.0)

Версия 2008 официально появилась 28 августа 2007 года.

26.1.5. Версия 2009 (16.0)

Интерфейс Norton Internet Security 2009

Версия 2009 официально появилась 8 сентября 2008 года. а[5]. Из новых функций можно отметить «белый список» файлов, основанный на репутации файлов[6]. Обновление вирусных баз занимает от 5 до 15 минут. В эту версию был интегрирован Norton Safe Web, предоставлявшийся ранее как отдельная услуга, зато была реинтегрирована фильтрация спама. По результатам тестов AV-Comparatives в феврале 2009 года Norton Internet Securty обнаружил 98,7 % вирусов и получил 3 звезды безопасности[7]. Но в эвристическом тесте NIS выловил только 35 % вирусов.

Системные требования для 32 битной Windows XP составляют: 300 МГц процессора, 256 Мб ОЗУ и 200 Мб свободного дискового пространства. Для 32 или 64 битной версии Windows Vista: 800 МГц процес-

сора, 512 Мб ОЗУ и 200 Мб свободного дискового пространства.

26.1.6. Версия 2010 (17.0)

Версию 2010 официально появилась 8 сентября 2009 года.

26.1.7. Версия 2011 (18.0)[8]

Версию 2011 официально появилась 31 августа 2010 года. Эта версия больше не поддерживает версии Windows ниже XP SP3. Изменения включают новый пользовательский интерфейс и улучшено сканирование интернет-сайтов на наличие вредоносных программ.

26.1.8. Версия 2012 (19.0)

Версия 2012 официально появилась 6 сентября 2011 года. В Norton Internet Security 2012 появились новые возможности. Одна из них Download Insight 2.0, в ней появилась новая возможность и теперь она показывает ещё и стабильность загруженного файла. Это означает, что если файл стабилен на Windows 7, но нестабилен на Windows XP, то пользователи Windows XP будут уведомлены что этот файл нестабилен на данной системе. Еще одна особенность - это обновлённый Sonar 4. Другим позитивным изменением является то, что Identity Safe и Safe Web, совместимы с Google Chrome. Пользовательский интерфейс также был упрощён.

26.2. История версий для MAC

26.2.1. 1.0 — 3.0

26.2.2. 4.0

Версия 4.0 была выпущена 18 декабря 2008 года[9][10]. В настоящее время брандмауэр блокирует вредоносные сайты, используя обновляемый черный список от Symantec. Из этой версии был исключен iClean. В этом выпуске была представлена хорошая защита от фишинга[11].

Системные требования: Mac OS X 10.4.11, PowerPC или Intel Core процессоров, 256 Мб ОЗУ и 150 Мб свободного дискового пространства.

26.3. Награды

- Gold Personal IDS/IPS Award (июнь 2011)[12]

26.4. Примечания

[1] Norton Internet Security 2009 16.2.0.7. Softpedia (February 3rd, 2009). Проверено 14 марта 2009. Архивировано из первоисточника 25 марта 2012.

[2] Norton Add-on Pack 2.1. Softpedia (July 14, 2008). Проверено 14 марта 2009. Архивировано из первоисточника 25 марта 2012.

[3] COMPANY NEWS; Symantec to Acquire Peter Norton. *Lawrence M. Fisher*. The New York Times Company (May 15, 1990). Проверено 30 марта 2009. Архивировано из первоисточника 25 марта 2012.

[4] The Norton Update Center. Symantec Corporation. Проверено 18 марта 2009. Архивировано из первоисточника 25 марта 2012.

[5] Symantec Launches Fastest Security Products in the World(недоступная ссылка — *история*). Marketwire, Incorporated (September 9, 2008). Проверено 4 марта 2009.

[6] Filtering Viruses Through The Cloud. *Andy Greenberg*. Forbes.com LLC (September 22, 2008). Проверено 11 марта 2009. Архивировано из первоисточника 25 марта 2012.

[7] Anti-Virus Comparative No. 21, February 2009. AV-Comparatives e.V.. Проверено 30 мая 2009. Архивировано из первоисточника 11 марта 2012.

[8] антивирусы.

[9] Symantec unveils Norton Internet Security for Mac 4.0. *Jim Dalrymple*. Mac Publishing, LLC (December 18, 2008). Проверено 27 марта 2009. Архивировано из первоисточника 25 марта 2012.

[10] Symantec releases Norton Internet Security for Mac 4.0. *Justin Berka*. Condé Nast Digital (December 19, 2008). Проверено 27 марта 2009. Архивировано из первоисточника 25 марта 2012.

[11] Norton Internet Security 4: A Comprehensive Suite. *John Martellaro*. The Mac Observer, Inc. (December 18th, 2008). Проверено 27 марта 2009. Архивировано из первоисточника 25 марта 2012.

[12] *Михаил Картавенко.* Тест персональных IDS/IPS на защиту от атак на уязвимые приложения (июнь 2012) - Тесты и сравнения антивирусов. *Anti-Malware.ru* (1 июня 2012). Проверено 10 июня 2012. Архивировано из первоисточника 10 июня 2012.

26.5. Ссылки

- Norton Internet Security

Глава 27

NPF

NPF (New Packet Filter) — межсетевой экран, разработанный в рамках проекта NetBSD.

Изначальной целью проекта была разработка фильтра (сетевых) пакетов, который, с одной стороны, будет воплощать в себе удобства и возможности PF, а с другой — будет легко расширяем и масштабируем на мультипроцессорных системах.

27.1. История

Первым разработчиком NPF является Mindaugas Rasiukevicius. Разработка NPF была спонсирована NetBSD Foundation. В репозиторий NetBSD код NPF вошёл 22 августа 2010 года, а первым релизом этой операционной системы со входящим в поставку NPF, является версия 6.0.

27.2. Особенности

Как и PF, NPF состоит из двух основных частей: одна располагается в ядре ОС и осуществляет собственно обработку пакетов, а другая — конфигурационная утилита npfctl. Синтаксис конфигурационных файлов и самой утилиты npfctl приближен к оному у pfctl, утилиты конфигурации PF. Однако собственно NPF представляет собой совершенно новый продукт.

NPF изначально создавался с учётом использования на мультипроцессорных системах и поэтому умеет использовать все доступные ядра/процессоры. NPF, в отличие от большинства других пакетных фильтров, не просто проходит по наборам правил, но компилирует их в специальный псевдокод, схожий с BPF.

27.3. Ссылки

- Введение NPF в NetBSD 6.0
- Руководство по конфигурационным файлам NPF

[1] http://bxr.su/n/sys/modules/npf/Makefile

[2] http://bxr.su/n/usr.sbin/npf/npfctl/Makefile

[3] http://bxr.su/n/usr.sbin/npf/npfctl/npf_parse.y

[4] http://bxr.su/n/usr.sbin/npf/npfctl/npf_scan.l

Глава 28

Online Armor

Online Armor (Online Armor Security Suite) — персональный файрвол для Microsoft Windows NT, продукт в настоящее время принадлежит компании Emsi Software GmbH, которая купила его у компании Tall Emu.

28.1. Варианты программы

- *Online Armor Premium* — основная версия программы. В рейтинге сайта matousec.com версия 4.0.0.44 имела результат 97 % и оценку уровня защиты «Excellent».[2] В тесте на способность системы HIPS защитить ядро Windows, проведённом сайтом anti-malware.ru в апреле 2009 года, Online Armor Personal Firewall Premium 3.0.0.190 вместе с Comodo Internet Security занял первое место, пройдя 9 тестов из 9[3].
- *Online Armor Free* — бесплатная версия (freeware), не включает ряд возможностей программы. Версия 4.0.0.35 Online Armor Free также была протестирована сайтом matousec.com и получила оценку 96% с уровнем защиты «Excellent».[2]
- *Online Armor++* — содержит все возможности *Online Armor* плюс включает в себя антивирус.
- *Online Armor AV+* с антивирусом Касперского. Продажа и поддержка в настоящее время прекращены, однако, до приобретения продукта компанией EmsiSoft, она активно развивалась.

28.2. Возможности программы

Основные возможности Online Armor Free

- Обновления
- Защита от выполнения
- Защита автозапуска
- Обычный режим
- Обнаружение кейлоггеров
- Защита от внешних воздействий
- Режим защиты ядра
- Управление доменами
- Защита от завершения
- Фаервол
- Контроль программ

Основные функции Emsisoft Online Armor Premium

- Режим онлайн-банкинга
- Обновления
- Экран файлов и реестра
- Защита от выполнения
- Защита автозапуска
- Обычный режим
- Обнаружение кейлоггеров
- Защита от внешних воздействий
- Техническая поддержка
- Режим защиты ядра
- Управление доменами
- Фишинг-фильтр
- Защита от завершения
- Фаервол
- Углубленный режим
- Импорт и экспорт настроек
- Защита от подмены DNS
- Контроль программ

28.3. Награды

- Gold Firewall Outbound Protection Award от Anti-Malware.ru (сентябрь 2011)[4]

28.4. Примечания

[1] http://www.emsisoft.ru/ru/software/oa/

[2] Results and comments - www.matousec.com (web.archive.org)

[3] *Илья Шабанов.* Сравнение HIPS антивирусов на предотвращение проникновения в ядро Microsoft Windows. *Anti-Malware.ru* (20 апреля 2009). Проверено 20 декабря 2013. Архивировано из первоисточника 20 декабря 2013.

[4] Тест фаерволов на защиту от внутренних атак (сентябрь 2011) - Тесты и сравнения антивирусов - Anti-Malware.ru

28.5. Ссылки

- Официальный сайт компании (англ.)

Обзоры

- *Андрей Крупин.* Огненные стены для "Висты". *Компьютерра-Онлайн* (22 октября 2008). Проверено 17 декабря 2011.

Глава 29

Outpost Firewall

Outpost Firewall — (персональный файрвол) программа для защиты компьютера от хакерских атак из Интернета от российской компании Agnitum. Кроме этого, Outpost обеспечивает блокировку загрузки рекламы и активного содержимого веб-страниц, и тем самым — их более быструю загрузку.

29.1. Варианты программы

Outpost Firewall — выпускается в двух вариантах: *Outpost Firewall Pro* (лицензия Shareware) и *Outpost Firewall Free* (лицензия Freeware). Бесплатная последний раз обновилась в апреле 2011 года, имеет урезанный набор функций по сравнению с версией *Pro*; кроме того, компания Agnitum не осуществляет техническую поддержку этой версии.

29.2. Возможности программы

- Фильтрация входящих и исходящих сетевых соединений
- Глобальные правила для протоколов и портов
- Создания правил сетевого доступа для известных приложений на основе предустановок
- Создания правил сетевого доступа и настройка параметров проактивной защиты для приложений в режиме автообучения
- Политики блокировки задают реакцию Outpost на соединение, отсутствующее в правилах — автоматически отклонить его, разрешить или выдать запрос на создание правила, кроме того, блокировка / разрешение всех соединений
- Контроль компонентов, контроль скрытых процессов и контроль памяти процессов позволяют устанавливать ограничения на сетевую активность для отдельных приложений и процессов, определяя, какие именно — входящие или исходящие — соединения разрешены для конкретных приложений
- Визуальное оповещение о событиях (например, о блокировании соединения, попытке сетевой атаки) с помощью всплывающих окон
- Наглядное отображение сетевой активности
- Журнал действий программы
- Внутренняя защита (например, от попыток остановить сервис) и возможность задать пароль на изменение конфигурации
- Технология **SmartDecision**, осуществляющая статический анализ запускаемых файлов, на основе множества критериев оценивает потенциальную угрозу и выводит подсказку пользователю о дальнейших действиях
- **ImproveNet** - "облачный" сервис, собирающий информацию о локальном взаимодействии приложений на компьютере. Эти новые правила автоматически обновляются у подписчиков ImproveNet и используются для различения вредоносной и безопасной активности
- **SmartScan** (кэширование статуса проверки) - технология, повышающая скорость проверки компьютера на наличие вредоносных объектов путем создания специальной базы, в которой хранится информация о уже проверенных "чистых" файлах, которые исключаются из проверки.
- Чтобы сократить количество запросов режима обучения, выдаваемых в течение первого времени работы Outpost Firewall Pro, **можно назначить продукту запоминать (самостоятельно изучать) типичную деятельность системы путем активации режима автообучения**. В этом режиме Outpost Firewall Pro предполагает, что деятельность программ с рейтингом "хорошее" и "доверенное" является законной, и, соответственно, разрешает доступ к сети и взаимодействие между процессами для таких программ. В то время, когда такие программы устанавливают соединение с Интернет и взаимодействуют с другими программами, Outpost Firewall

Pro запоминает их параметры и создает разрешающие правила для всех запрошенных соединений. Согласно этим правилам программы смогут устанавливать соединения после окончания периода автообучения и возвращения продукта к обычному режиму отслеживания сетевой активности, а пользователь уже не будет получать соответствующих запросов - если для запрашиваемого соединения уже существует правило, оно будет определять параметры данного соединения.

29.3. Компоненты Outpost Firewall

В состав дистрибутива Outpost Firewall Pro входят следующие модули:

- *Web-контроль* — позволяет блокировать интернет-рекламу по ключевым словам и типичным размерам рекламных баннеров. Возможен контроль над следующими элементами: ActiveX, приложения Java, программы на основе сценариев Java и Visual Basic, cookies, всплывающие окна, сценарии ActiveX, внешние интерактивные элементы, referrers, скрытые фреймы, GIF- и flash-анимации. Списки опасных сайтов обновляются в рамках программы ImproveNet.
- *Детектор атак* — обнаруживает и блокирует попытки сетевых атак
- *Фильтрация почтовых вложений* — обнаруживает и переименовывает потенциально опасные вложения в электронной почте
- *Anti-Leak* — не допускает действий опасных программ и полностью защищает от троянцев, шпионского ПО и других угроз, используя технологии Контроля компонентов (**Component Control**), Контроля Anti-Leak (**Anti-Leak Control**) и Защиты системы (**System Guard**). Anti-Leak обеспечивает первую линию обороны от вредоносного ПО, проактивно контролируя поведение и взаимодействие приложений на персональном компьютере.

29.4. Награды

- Outpost Firewall Pro был признан лучшим продуктом 2008 года в категории *персональный брандмауэр* по версии журнала Мир ПК [1]
- 21-12-2010 в тесте Proactive Security Challenge на сайте http://www.matousec.com Outpost Security Suite Free занял третье место с результатом 97 % и оценкой «Excellent» Level reached 10+. Рекомендован к применению. http://www.matousec.com/projects/proactive-security-challenge/results.php

29.5. Ссылки

- Официальный сайт компании Agnitum

29.6. Примечания

[1] Лучший продукт 2008

Глава 30

Packet Filter

Pa´cket Fi´lter (PF) — файрвол, разрабатываемый в рамках проекта OpenBSD. Обладает высокой скоростью работы, удобством в конфигурировании и большими возможностями, включая поддержку IPv6. На данный момент используется, помимо OpenBSD, в NetBSD и FreeBSD, а также основанных на этих трёх MirOS BSD, DesktopBSD, pfSense и других. Начиная с версии 10.7 PF используется в Mac OS X. PF был портирован на Microsoft Windows и лёг в основу файрвола Core Force[4].

30.1. История

История PF началась в 2000 году, когда Даррен Рид, разработчик использовавшегося в то время в OpenBSD файрвола IPFilter, изменил лицензию на него. Тогда ipf был исключён из CVS-репозитория, а его место к релизу OpenBSD 3.0 занял написанный «с нуля» PF.

В OpenBSD 3.3 появился pfsync — псевдоинтерфейс, позволяющий реплицировать информацию о контексте соединений между двумя (а позднее и больше) хостами. При использовании CARP или другой аналогичной технологии pfsync позволяет, в частности, создавать отказоустойчивые конфигурации из нескольких физических межсетевых экранов: при отказе одного хоста второй продолжит обрабатывать сетевой трафик без разрыва соединений.

Изначально PF был довольно похож на IPFilter. Крупный редизайн внутренней архитектуры начался в 2005 году[5] усилиями Хеннинга Брауэра и Райана Макбрайда. В рамках этого проекта PF получил поддержку нового вида правил *match*, новую схему учёта контекста соединений (англ. *states* в оригинальной терминологии). Так же крупным изменением стал отказ от разделения наборов правил по типам: ранее PF, как и IPFilter, имел раздельные наборы правил для NAT и фильтрации трафика. Так же, в рамках общего развития OpenBSD, PF получил поддержку множественных таблиц и доменов маршрутизации.

30.2. Архитектура

PF состоит из двух частей: собственно фильтра пакетов[6] и утилиты pfctl,[7] которая предоставляет интерфейс для управления межсетевым экраном. Фильтр полностью работает в контексте ядра операционной системы, взаимодействие с ним осуществляется через системный вызов ioctl.[8] Поэтому pfctl, строго говоря, не является необходимой частью PF.

PF изначально не рассчитан на многопоточную обработку пакетов. С другой стороны, отсутствие блокировок положительно влияет на производительность.

30.2.1. Оптимизация

PF умеет пропускать ненужные проверки во время прохождения списка правил. Например, если два правила подряд относятся только к протоколу TCP, то пакет любого другого протокола (например, UDP), после того как не подойдёт к первому правилу, не будет проверяться на втором. Для этого сначала при составлении набора правил pfctl, зная наиболее оптимальный порядок проверок, может изменить взаимный порядок нескольких идущих подряд правил; затем подготовленный набор анализируется при загрузке в PF и для каждого правила составляется карта переходов по несовпадению того или иного параметра.

PF при оптимизации списка правил может также учитывать накопившуюся статистику частоты проверок для правил, и корректировать карту переходов в соответствии с этой статистикой.

30.3. Порядок работы

Фильтр обрабатывает сетевые пакеты в один (при посылке пакета с того же компьютера, на котором стоит фильтр, на другой компьютер, или наоборот) или два (при пересылке внутри компьютера или когда компьютер с фильтром исполняет роль сетевого шлюза) цикла обработки.

Собственно обработка пакета происходит согласно набору правил. В финале обработки пакет либо отбрасывается, либо пропускается. Каждое правило состоит из набора условий и набора указаний, выполняемых при удовлетворении набора условий. Правила бывают трёх видов:

match Если пакет удовлетворяет условиям правила, то указания из данного правила выполняются моментально. match-правила обычно используются для NAT, журналирования трафика, QoS и так далее.

block Если пакет не удовлетворяет условиям правила, то он помечается как подлежащий блокировке. PF позволяет как просто отбросить пакет, так и сгенерировать ICMP-сообщение об ошибке.

pass Если пакет удовлетворяет условиям правила, то он помечается как подлежащий пропуску далее.

Указания, записанные для block- и pass-правил, выполняются после завершения прохода по набору правил. Если для block- или pass-правила сделана соответствующая пометка, то при удовлетворении пакетом условий данного правила, проход по набору правил будет прерван с выполнением соответствующих указаний. Такой порядок позволяет задать серию правил, постепенно сужающих область применения, что выглядит более естественно, чем обратный порядок. Если ни одно block- или pass-правило не подошло, то пакет пропускается: это мера защиты от случайной ошибки при конфигурировании сетевого экрана.

Правила могут включать в себя следующие указания:

нормализация сборка фрагментированных и отбрасывание заведомо некорректных пакетов, а также другие операции, упрощающие дальнейшую обработку;

трансляция перенаправление трафика на уровнях 2 (более тонкое, чем его могут обеспечить обычные средства маршрутизации) и 3 модели OSI, с поддержкой NAT и пулов адресов назначения;

приоритизация принудительное выставление типа обслуживания пакета, помещение пакета в ту или иную очередь ALTQ;

фильтрация принятие окончательного решения о пропуске или блокировке сетевого пакета.

30.3.1. Возможности фильтрации

PF умеет фильтровать пакеты по следующим параметрам:

- Сетевой адрес (для TCP и UDP также и порт) источника и получателя пакета
- Сетевой интерфейс (или их группа), на котором обрабатывается пакет, а также на котором он изначально появился в системе
- Корректность маршрута, с которого пришёл пакет (да или нет)
- Флаги (для TCP)
- Биты типа обслуживания (*ToS*)
- Тип и код ICMP (для ICMP и ICMPv6)
- Теги пакетов
- Локальный пользователь (владелец сокета)
- Различные счётчики соединений
- Вероятность

Последний параметр позволяет создавать правила, которые срабатывают «иногда», что помогает бороться с (порой непреднамеренными) DDoS-атаками.

Теги назначаются правилами PF. У каждого пакета может быть не более одного тега. Правилом можно установить/заменить тег, но нельзя убрать существующий. Тег сохраняется у пакета на всё время прохождения по сетевому стеку.

PF также позволяет переопределить используемую таблицу маршрутизации, за счёт чего можно переносить пакеты между доменами маршрутизации. Разумеется, это имеет смысл только для входящего трафика, для которого маршрут ещё не определён стандартными средствами.

Для правил можно указывать *метки*. Одна и та же метка может соответствовать нескольким правилам. Метки позволяют лучше идентифицировать правила из пользовательского пространства, а также отключать встроенную оптимизацию набора правил для определённых правил; последнее может быть нужно, например, для биллинговых систем.

PF не только умеет проводить фильтрацию с учётом контекста, но поддерживает три варианта работы в этом режиме (терминология из оригинальной документации):

keep state простой режим, запоминается только соответствие пар сетевых адресов и портов; этот режим применим не только к TCP, но и к UDP.

modulate state более сложный режим, в котором PF самостоятельно выбирает начальные значения счётчиков пакетов TCP; это обеспечивает улучшенную защиту в случаях, когда одна из сторон выбирает плохие с точки зрения вероятности угадывания значения этих счётчиков.

synproxy state в этом режиме PF самостоятельно устанавливает TCP-соединение с другой стороной, и только после этого соответствующие пакеты отсылаются инициатору; это обеспечивает защиту от атак типа SYN-флуд с подделкой адреса отправителя.

По умолчанию все pass-правила учитывают контекст (keep state), а относящиеся к TCP ещё и проверяют флаги SYN-пакета. Это сделано поскольку позволяет заметно сократить объём правил (как в плане их количества, так и в плане их описания в файле конфигурации) в типичных ситуациях. При этом можно принудительно отказаться от этих возможностей для конкретного правила или всего их набора. Следует также учитывать, что если пакет не попал ни под одно pass-правило, то никаких проверок и создания контекста не происходит.

30.4. Таблицы адресов

Одной из самых интересных возможностей PF является работа с таблицами адресов:

- Таблицы могут содержать как IPv4-, так и IPv6-адреса, вместе с маской подсети для каждого;
- Записи в таблице могут быть быть помечены как исключение, что позволяет кратко описывать сложную топологию (см. ниже);
- Поиск по таблице происходит быстрее, чем линейный поиск по набору адресов (и заметно быстрее, чем перебор правил, различающихся лишь адресами в одном и том же параметре);
- Таблицы могут быть произвольным образом изменены без необходимости перезагружать правила;
- По каждой записи в таблице может вестись статистика;
- Посредством опции фильтрации *overload* в выбранную таблицу могут помещаться адреса, превышающие те или иные ограничения на количество соединений;
- Записи в таблицах могут быть автоматически удалены по достижении указанного времени их существования.

Например, в таблицу можно занести все приватные адреса[9][10][11] в единую таблицу и затем блокировать попытки подключения извне от якобы этих адресов всего одним правилом.

Более того, путём использования пометок об исключении адресов (диапазонов адресов) можно путём всего трёх записей в таблице указать такую конфигурацию: в таблицу входит диапазон 10.0.0.0/8, кроме 10.0.3.192/26, плюс ещё входит 10.0.3.211. Соответствующие записи в таблицу можно заносить в любом порядке, PF будет их использовать в соответствии с их префиксами (маской подсети).

Сторонние программы через системный вызов ioctl или посредством вызова программы pfctl могут управлять содержимым таблиц. Например, DHCP-сервер dhcpd из состава OpenBSD поддерживает использование до трёх таблиц PF:

- таблица, в которую добавляются IP-адреса новых DHCP-клиентов
- таблица, из которой удаляются освобождающиеся IP-адреса
- таблица, в которой поддерживается список временно запрещённых к использованию IP-адресов

30.5. Блоки правил

Правила можно объединять в блоки (*anchors* в оригинальной документации). При этом можно для каждого блока задавать общие параметры, которые будут действовать для всех правил в блоке.

Блоки обрабатываются наравне с правилами и могут вкладываться друг в друга. При этом содержимое блоков может изменяться независимо друг от друга, а также от общего списка правил. Последний, по сути, является тем же блоком.

Блоки правил удобны для использования в программах, так или иначе управляющих потоками трафика. Примеры программ:

- relayd, прокси-сервер для организации автоматического контроля списка работающих backend-серверов;
- authpf, командная оболочка UNIX, позволяющая контролировать доступ к сетевым ресурсам при помощи аутентификации пользователей через SSH.

30.6. Литература

- *Майкл Лукас.* Absolute OpenBSD. — No Starch Press, 2003. — 500 с. — ISBN 1-886411-99-9.
- *Ясек Артимьяк (англ.* Jacek Artymiak*).* Building Firewalls with OpenBSD and PF. — 2-е изд. — No Starch Press, 2003. — 320 с. — ISBN 83-916651-1-9.

- *Брэндон Палмер, Жосе Назарио.* Secure Architectures with OpenBSD. — Addison-Wesley Professional, 2004. — 520 с. — ISBN 0-321-19366-0.

- Более полный список книг доступен на соответствующей странице сайта OpenBSD.

- Перевод книги о PF. Второе издание доступно здесь или здесь.

30.7. Примечания

[1] http://openbsd.su/src/sys/net/

[2] http://openbsd.su/src/sbin/pfctl/

[3] http://openbsd.su/src/sbin/pfctl/parse.y

[4] Сетевой экран Core Force для Microsoft Windows 2000/XP

[5] *Henning Brauer.* «Placeholder: something OpenBSD related» (слайд 6). Архивировано из первоисточника 14 февраля 2012.

[6] страница руководства pf(4)

[7] страница руководства pfctl(8)

[8] страница руководства ioctl(2)

[9] RFC 1918 (приватные адреса в Интернет)

[10] RFC 3927 (адреса для Zeroconf)

[11] IP Filter HOWTO, содержит хороший список приватных адресов с пояснениями

30.8. Ссылки

- Официальная документация

- Руководство FreeBSD: PF, межсетевой экран OpenBSD

- Учебник по FreeBSD, OpenBSD, NetBSD, DragonFly (BSDA в вопросах и ответах): fw

Глава 31

Panda Cloud Antivirus

Panda Cloud Antivirus — антивирусное программное обеспечение с функциями брандмауэра, разрабатываемое Panda Security. Продукт был представлен весной 2009 года CEO компании Хуаном Сантана в качестве защитного решения с новой моделью защиты, использующей облачные вычисления[1]. Программа предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, червей, adware и дозвонщиков. На ноябрь 2011 года серверы «Коллективного Разума» (англ. *Collective Intelligence*) Panda Cloud Antivirus проанализировали более 200 млн файлов[2].

31.1. Особенности

Главной особенностью антивируса является то, что он распространяется по принципам «Программное Обеспечение + Услуги» *(англ. S+S — Software plus Services)*, то есть пользователь устанавливает на свой компьютер программу, а часть работы программы происходит на серверах Panda Security (детектирование на локальном компьютере и сканирование с использованием облачных технологий)[3][4]. Таким образом, достигается высокая эффективность антивируса при низкой нагрузке на систему[5][6].

31.1.1. Работа антивируса

Антивирус Panda Cloud работает, используя вычислительные способности локального компьютера и удалённых серверов Panda Security. В облаке антивирус пользуется системой Collective Intelligence, собирающей, анализирующей, категоризирующей и выполняющей лечение файлов. Все сигнатуры вредоносного ПО находятся именно на удалённых серверах, избавляя пользователя от необходимости загружать их обновления. На пользовательской стороне работает эвристический анализатор и инструменты постоянного сканирования, которые имеют три степени приоритета[3]:

- **Мгновенное сканирование** — антивирус проверяет все активные процессы, программы и файлы.
- **Сканирование с упреждающей выборкой** — антивирус откладывает сканирование файлов, загруженных из Интернета или с внешних носителей, но не запущенных пользователем, на то время, пока не совершатся рутинные действия с высоким приоритетом. Если пользователь начнёт работать с данными файлами, то они будут перенесены в категорию для мгновенного сканирования.
- **Фоновое сканирование** — антивирус в фоновом режиме сканирует все файлы системы, пока пользователь не работает с компьютером.

При сканировании антивирус может создавать особые кэши, которые позволяют при повторном сканировании значительно сократить время проверки компьютера[7]. Также антивирус способен контролировать посещения сайтов пользователем, блокируя вредоносные[8][9].

31.2. Сертификации и награды

- ICSA Labs сертифицировала антивирус Panda Cloud как соответствующий стандартам[10].
- Microsoft присвоила антивирусу статус «Совместим с Windows 7»[11].
- Издание PCMag дважды наградила антивирус званием «Выбор редакторов» в номинации «Лучший бесплатный антивирус»[12][13].
- Китайская антивирусная лаборатория PCSecurityLabs вручила сертификат о высокой эффективности антивируса[14].
- Лаборатория AV-Comparatives в августе 2011 года присвоила антивирусу высшую награду (*Advanced+*) с уровнем обнаружения вредоносного ПО в 99,3 % в категории *«сканирование по запросу»*[15], а в ноябре 2011 года награду II степени (*Advanced*) с уровнем обнаружения 41,4 %

при низком уровне ложных срабатываний в категории *«Обнаружение неизвестного вредоносного ПО»*[16].

- Обозреватель румынского портала Softpedia Ионат Иласку отметил, что антивирус прост в использовании, непритязателен к системным ресурсам, обеспечивая безопасность от большинства существующих типов вредоносного ПО, хотя при этом, обладая высокой степенью обнаружения, антивирус не может справиться с нейтрализацией некоторых угроз. По итогам обзора редактор сайта присвоил антивирусу пять баллов из пяти возможных (англ. *excellent*)[17].

31.3. Примечания

[1] *Byron Acohido.* Panda Cloud Antivirus hits Internet for free (англ.). USA Today (29 April 2009). — «"The threat climate demands a new protection model," Santana says.» Проверено 24 ноября 2011. Архивировано из первоисточника 6 июля 2012.

[2] *Taylor Armerding.* Panda process 200 millionth piece of cloud-based malware (англ.). ComputerWorld UK (14 November 2011). Проверено 24 ноября 2011. Архивировано из первоисточника 6 июля 2012.

[3] *Pedro Bustamante.* New Protection Model Explained (англ.). Panda Security (29 апреля 2009). — «With Panda Cloud Antivirus we introduce a new protection model based on a thin-client agent & server architecture» Проверено 13 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[4] *Marius Oiaga.* Download Free Panda Cloud Antivirus Beta (англ.). Softpedia. — 30 апреля 2009. Проверено 12 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[5] *Сергей и Марина Бондаренко.* Panda Cloud Antivirus - антивирус с минимальным потреблением ресурсов (рус.), *Daily Digital Digest* (30 апреля 2009). Проверено 12 декабря 2010.

[6] *Seth Rosenblatt.* Panda Cloud Antivirus Free Edition 1.3 (англ.). CNET (27 октября 2010). Проверено 12 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[7] *Steve Ragan.* Panda Cloud Antivirus 1.0 Review (англ.). The Tech Herald.com (13 ноября 2009 года). — «As mentioned, the first scan is slowest. After that, the scans will get faster as the CloudAV cache builds up.» Проверено 24 декабря 2010. Архивировано из первоисточника 11 мая 2012.

[8] *Steve Ragan.* Panda Cloud Antivirus 1.0 Review (англ.). The Tech Herald.com (13 ноября 2009 года). — «This site attempts to install a Rogue anti-Virus called AntiAID. The installation file was blocked by Panda as Sinowal.gen.» Проверено 24 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[9] *Lucian Constantin.* New Panda Cloud Antivirus Version Released (англ.), *Softpedia News* (October 27th, 2010, 16:55 GMT). Проверено 24 декабря 2010. «Detection wise, the most important new feature of Panda Cloud Antivirus 1.3 is the Web filtering component, which leverages the company's threat intelligence services to block malicious websites.».

[10] Panda Cloud Antivirus (англ.). ICSALabs. Проверено 13 декабря 2010.

[11] Panda Cloud Antivirus (англ.). Microsoft Corp.. Проверено 13 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[12] *Neil J. Rubenking.* Panda Cloud Antivirus Free Edition 1.0 (англ.). PCMag (13 ноября 2009). — «Panda Cloud Antivirus offers free malware protection in a lightweight package with an ultra-fresh user interface.» Проверено 13 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[13] *Neil J. Rubenking.* Panda Cloud Antivirus 1.1 (англ.). PCMag (9 июня 2010). — «This free antivirus is great at keeping malicious software from installing on clean computers. It's less effective at cleaning up existing infestations, so, if it detects a threat, run another product for a second scrubbing.» Проверено 13 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[14] Greater China Region Protection Certificate (англ.). PC Security Labs (Beijing, China) (15 сентября 2010). — «Panda Cloud Antivirus launched by Panda Security is delivering a high standard of comprehensive protection to users in the Greater China region along with a low false positive level.» Проверено 13 декабря 2010. Архивировано из первоисточника 6 июля 2012.

[15] On-Demand Comparative August 2011 (англ.) (PDF). AV-Comparatives e. V. (27 September 2011). Проверено 24 ноября 2011. Архивировано из первоисточника 6 июля 2012.

[16] Retrospective Test November 2011 (англ.) (PDF). AV-Comparatives e. V. (15 November 2011). Проверено 24 ноября 2011. Архивировано из первоисточника 6 июля 2012.

[17] *Ionut Ilascu.* Panda Cloud Antivirus Nimbler than Ever (англ.). Softpedia (22 June 2011). Проверено 31 июля 2011. Архивировано из первоисточника 31 июля 2011.

31.4. Ссылки

31.4.1. Официальные сайты

- Официальный сайт (рус.)
- Официальный форум (англ.)

31.4.2. Обзоры в прессе

- *Neil J. Rubenking.* Panda Cloud Antivirus Free Edition 1.0 (англ.). PC Magazine (13 ноября 2009). — «Panda Cloud Antivirus offers free malware protection in a lightweight package with an ultra-fresh user interface.» Проверено 12 декабря 2010. Архивировано из первоисточника 11 мая 2012.
- *Seth Rosenblatt.* Panda Cloud Antivirus Free Edition 1.3 (англ.). CNET (27 октября 2010). — «Panda Cloud Antivirus makes a decent, reasonable security choice for anybody looking to effectively balance security and system performance.» Проверено 18 декабря 2010. Архивировано из первоисточника 11 мая 2012.
- *Mark Wilson.* Panda Cloud Antivirus review (англ.). TechRadar (7 марта 2010). — «Panda Cloud Antivirus approaches virus protection from a different angle» Проверено 18 декабря 2010. Архивировано из первоисточника 11 мая 2012.
- *Steve Ragan.* Panda Cloud Antivirus 1.0 Review (англ.). The Tech Herald (13 ноября 2009). — «With that said, CloudAV scored an 85 out of 90. CloudAV is clean looking, fast, and free.» Проверено 24 декабря 2010. Архивировано из первоисточника 11 мая 2012.
- *Ionut Ilascu.* Panda Cloud Antivirus Pro (англ.). Softpedia (4 июня 2010). — Windows software reviews. — «It preserves ease of use and minimalist interface, while also time enforcing protection with behavioral detection. Shutting off possible malware entry points, such as Windows Autorun and USB drive's autorun.inf, makes for valid proactive measures against threats.» Проверено 24 декабря 2010. Архивировано из первоисточника 11 мая 2012.
- *Андрей Крупин.* "Облачный" антивирус (рус.). Компьютерра-Онлайн (07 мая 2009 года). Проверено 18 декабря 2010.

31.4.3. Дополнительно

- *Lenny Zeltser.* What Is Cloud Anti-Virus and How Does It Work (англ.). Lenny Zeltser (6 октября 2010). — Объяснение принципов работы облачных антивирусов со ссылкой на академические круги. — «Defining Cloud Anti-Virus» Проверено 24 декабря 2010. Архивировано из первоисточника 11 мая 2012.

Глава 32

PC Tools Firewall Plus

PC Tools Firewall Plus — бесплатный персональный межсетевой экран компании PC Tools для ОС Windows XP, Windows Vista и Windows 7. В настоящее время в виде отдельного продукта не выпускается, а включен в состав PC Tools Internet Security.

32.1. Возможности программы

- Фильтрация входящих и исходящих сетевых соединений.
- Глобальные правила для протоколов и портов, устанавливаемые отдельно для каждой сети.
- Создание правил сетевого доступа для известных приложений.
- Создание правил для приложений имеющих действительную цифровую подпись.
- Контроль компонентов, контроль скрытых процессов и контроль памяти процессов.
- Установка ограничений на сетевую активность для отдельных приложений и процессов отдельно для входящих и исходящих соединений.
- Визуальное оповещение о событиях с помощью всплывающих окон.
- Наглядное отображение сетевой активности с помощью анимированного значка в области уведомлений.
- Журнал действий программы.
- Отображение информации о сетевой активности каждого приложения.
- Два режима работы: простой и продвинутый.

32.2. Позиции в рейтингах программ класса «Firewall»

На сайте **matousec.com**, посвящённом проблемам защиты персонального компьютера программами класса Firewall, PC Tools Internet Security 2011 8.0.0.655 в тесте Proactive Security Challenge имеет результат 90 % и оценку «Very Good». Рекомендован к применению.[2]

Версия PC Tools Internet Security 2012 9.0.0.898 в тесте Proactive Security Challenge 64 имеет результат 6 % и оценку «None». Не рекомендован к применению.[3]

32.3. Примечания

[1] в составе PC Tools Internet Security

[2] Proactive Security Challenge (англ.)

[3] Proactive Security Challenge 64 (англ.)

32.4. Ссылки

Обзоры

- *Андрей Крупин.* Огненные стены для "Висты". *Компьютерра-Онлайн* (22 октября 2008). Проверено 17 декабря 2011.

Глава 33

pfSense

pfSense — дистрибутив для создания межсетевого экрана/маршрутизатора, основанный на FreeBSD. pfSense предназначен для установки на персональный компьютер, известен своей надежностью и предлагает функции, которые часто можно найти только в дорогих коммерческих межсетевых экранах. Настройки можно проводить через web-интерфейс что позволяет использовать его без знаний базовой системы FreeBSD. pfSense обычно применяется в качестве периметрового брандмауэра, маршрутизатора, сервера DHCP/DNS, и в качестве VPN hub/spoke.

Название происходит от факта, что pfSense помогает использовать инструмент фильтрации пакетов pf из OpenBSD более осознанно для непрофессиональных пользователей.

33.1. История

Проект pfSense возник в 2004 году как форк популярного дистрибутива m0n0wall авторами Chris Buechler и Scott Ullrich. С самого начала он был нацелен на полную установку на компьютер, в противовес нацеленности m0n0wall на встраиваемые системы. Тем не менее, pfSense доступен так же в виде образа для встраиваемых систем на основе CompactFlash. Версия 1.0 была выпущена 4 октября 2006.

На данный момент идет разработка версии 2.1, которая принесет массу улучшений. Включая инструменты для централизованного управления большим количеством pfSense систем. Версия 2.1 содержит полную поддержку IPv6 в основных сервисах.

33.2. Возможности pfSense

- Firewall
- State Table
- NAT — Network Address Translation
- Redundancy — два или более файрвола могут быть объединены в отказоустойчивую группу, также поддерживается синхронизация настроек между ними
  - CARP — CARP из OpenBSD позволяет создать аппаратную защиту от сбоев. Два или более межсетевых экрана могут быть объединены в отказоустойчивую группу. В случае отказа сетевого интерфейса на главном межсетевом экране, активным становится другой. Так же pfSense предоставляет возможность синхронизации настроек: если изменены настройки на одном фаерволе, то они автоматически будут синхронизированы на другом.
  - pfsync — pfsync обеспечивает репликацию состояния фаерволов. Это означает, что все существующие сетевые соединения сохранятся при выходе из строя одного из фаерволов, что очень важно для обеспечения отказоустойчивости сети.
- Outbound and Inbound Load Balancing обеспечивается подключение к нескольким провайдерам с равномерным распределением трафика между ними (пользователь, открывающий web страницу не замечает, что элементы этой страницы загружаются по разным каналам)
- VPN сервер — IPsec, OpenVPN, PPTP
- PPPoE сервер
- Динамический DNS
- DHCP сервер и шлюз
- Прокси сервер
- Captive portal — перенаправление на специальную веб-страницу для авторизации для доступа в Интернет
- Мониторинг и графические отчеты с использованием RRD
- Работа в режиме LiveCD
- Поддержка программных модулей.

Наиболее значимые расширения:

- Squid — прокси-сервер
- Snort — система обнаружения/нейтрализации вторжений.

33.3. Требования к аппаратному обеспечению pfSense

При разворачивании системы с ожидаемой пропускной способностью менее **10** Мбит/с минимальные требования к системе: процессор с тактовой частотой 100 МГц или больше, оперативная память 128 Мб или больше.

Система с пропускной способностью в **200** Мбит/с потребует: процессор с тактовой частотой 1000 МГц, оперативной памяти минимум 512 Мб.

Для пропускной способности до **500** Мбит/с потребуется: процессор с тактовой частотой 2000-3000 МГц, оперативная память 1024 Мб или больше.

Для развёртывания системы со скоростью передачи данных в **1000** Мбит/с между двумя интерфейсами, может быть использован Pentium 4 с частотой 3000 МГц или более быстрый, с PCI-X или PCI-e адаптером, т.к. ограничения шины PCI будут препятствовать повышению производительности между двумя 1 Гбитными адаптерами. Оперативная память 2048 Мб или более.

Требования к количеству оперативной памяти предъявляются в зависимости от поставленных задач. Например: требуется организовать безусловный совместный доступ в Интернет небольшого предприятия при скорости передачи данных к провайдеру 100 Мбит/с. Достаточной конфигурацией будет: процессор 1 ГГц, оперативная память 256 Мб. Всё то же самое + выход в Интернет через прокси сервер с ведением статистики: - объём оперативной памяти желательно увеличить до 512 Мб.

33.4. История релизов

- 4 октября 2006 года — pfSense version 1.0[1].
- 20 октября 2006 года — pfSense version 1.0.1[2].
- 25 февраля 2008 года — pfSense version 1.2[3].
- 26 декабря 2008 года — pfSense version 1.2.1[4].
- 7 января 2009 года — pfSense version 1.2.2[5].
- 10 декабря 2009 года — pfSense version 1.2.3[6].
- 17 сентября 2011 года — pfSense version 2.0[7]
- 20 декабря 2011 года — pfSense version 2.0.1[8]
- 21 декабря 2012 года — pfSense version 2.0.2[9]
- 15 апреля 2013 года — pfSense version 2.0.3[10]
- 15 сентября 2013 года — pfSense version 2.1.0[11]
- 4 апреля 2014 года — pfSense version 2.1.1[12]
- 10 апреля 2014 года — pfSense version 2.1.2[13]
- 2 мая 2014 года — pfSense version 2.1.3[14]
- 25 июня 2014 года — pfSense version 2.1.4[15]
- 27 августа 2014 года — pfSense version 2.1.5[16]
- 23 января 2015 года — pfSense version 2.2[17]
- 17 марта 2015 года — pfSense version 2.2.1[18]
- 15 апреля 2015 года — pfSense version 2.2.2[19]
- 27 июня 2015 года — pfSense version 2.2.4[20]
- 4 ноября 2015 года — pfSense version 2.2.5[21]

33.5. См. также

- m0n0wall
- PF
- IPCop

33.6. Примечания

[1] pfSense Digest: pfSense 1.0 RELEASED!
[2] pfSense Digest: pfSense 1.0.1 RELEASED!
[3] pfSense Digest: 1.2 Release Available!
[4] pfSense Digest: 1.2.1 Release Available!
[5] pfSense Digest: 1.2.2 Release Available!
[6] pfSense Digest: 1.2.3 Release Available!
[7] pfSense Digest: 2.0 Release Now Available!
[8] pfSense Digest: 2.0.1 release now available!
[9] pfSense Digest: 2.0.2 Release Now Available!
[10] pfSense Digest: 2.0.3 Release Now Available!
[11] pfSense 2.1-RELEASE now available!
[12] 2.1.1-RELEASE now available!
[13] 2.1.2 Release Now available!
[14] 2.1.3 Release Now available!
[15] 2.1.4 Release Now available!

[16] 2.1.5 Release Now available!

[17] 2.2-RELEASE Now Available!

[18] 2.2.1 RELEASE Now Available!

[19] pfSense Digest » 2.2.2-RELEASE Now Available!. blog.pfsense.org. Проверено 7 ноября 2015.

[20] 2.2.2 RELEASE Now Available!

[21] pfSense Digest » 2.2.5-RELEASE Now Available!. blog.pfsense.org. Проверено 7 ноября 2015.

33.7. Ссылки

- Официальный сайт проекта pfSense (англ.)
- pfSense Features (англ.)
- pfSense Screenshots (англ.)
- PF: The OpenBSD Packet Filter (англ.)
- Review & configuration tutorial at Free Software Magazine (англ.)
- DIY pfSense firewall system beats others for features, reliability, and security at TechRepublic (англ.)
- Обзоры по настройке pfSense
- Практические решения в картинках на русском языке pfSense (рус.). Осторожно — сайт заполнен adware (рус.)!

Глава 34

Shorewall

Shorewall или более точно **Shoreline Firewall** — инструмент для настройки файрвола в Linux, программное обеспечение под свободной лицензией GNU GPL[1]. Технически является надстройкой над подсистемой Netfilter (iptables/ipchains) ядра Linux и обеспечивает упрощённые методы конфигурирования данной подсистемы. Используя аналогию для программистов: shorewall в сравнении с ipchains/iptables, то же, что язык C в сравнении с ассемблером. Он предоставляет более высокий уровень абстракции для описания правил работы файрвола.

34.1. Механизм работы

Программа не является демоном, то есть не работает постоянно. Правила хранятся в текстовых файлах, при запуске shorewall считывает свои файлы конфигурации и преобразует их в настройки понятные ipchains/iptables, после чего данные настройки файрвола могут действовать до перезапуска операционной системы. Shorewall не предусматривает GUI для конфигурирования, правка конфигурационных файлов может быть произведена в любом текстовом редакторе, но есть например модуль к системе Webmin для настроек через веб-интерфейс.

34.2. История проекта

Первая версия shorewall появилась в 1999 году. Основной разработчик и бессменный лидер проекта — Томас Истеп (Thomas M. Eastep).

34.3. Текущая версия

Последняя стабильная версия на сегодня — 4.6.13.1 от 18 сентября 2015. Начиная с версии 4, shorewall использует компилятор правил основанный на Perl, ранее использовался более медленный компилятор на базе shell. Также с версии 4.2.4 поддерживается IPv6. Есть средства для клонирования настроек на несколько компьютеров, для упрощения конфигурирования больших сетей.

34.4. Достоинства и недостатки

Хотя синтаксис, предлагаемый shorewall, выглядит проще, чем синтаксис оригинальных правил iptables/ipchains, но настройка в текстовых файлах может оказаться затруднительной человеку непосвящённому в работу файрвола в Linux. Область применения shorewall больше ориентирована на системных администраторов и настройку серверов, нежели на пользователей десктопов. Однако для системных администраторов схема настройки через текстовые файлы может быть даже более удобной, нежели необходимость GUI, поскольку настройку shorewall можно произвести лишь при наличии текстовой консоли или ssh/ftp соединения с сервером.

Документации по shorewall на русском языке немного и она преимущественно по старым версиям программы, это может быть дополнительным препятствием к использованию русскоязычными пользователями. Разумеется, для профессиональных системных администраторов, на которых и ориентирован shorewall, отсутствие документации на национальном языке не является существенной проблемой.

34.5. Распространённость и пути получения

Shorewall входит в ряд дистрибутивов Linux (например в Debian, Gentoo и др.). Исходные тексты можно также получить с официального сайта проекта. Автор предупреждает, что канал в интернет с официального сайта слабый и рекомендует пользоваться региональными зеркалами для получения исходных текстов. Официальное зеркало[2] в рунете — http://shorewall.ru (Не работает).

34.6. См. также

34.7. Примечания

[1] Shoreline Firewall (Shorewall)

[2] Shorewall Mirrors

34.8. Ссылки

- Сайт проекта (англ.)
- Зеркало сайта проекта в рунете (Не работает) (англ.)
- Архив почтовых рассылок Shorewall (англ.)

Глава 35

TMeter

TMeter — интернет-шлюз для операционной системы Microsoft Windows. Основные задачи программы — организация доступа в Интернет, подсчет трафика, ограничение скорости, запрет доступа к вебсайтам на основе «черных списков». Существует полностью бесплатная редакция TMeter Freeware Edition (отсутствует триальный срок), которая позволяет использовать только три фильтра учёта трафика.

35.1. Особенности программы

- NAT
- Гибкая система подсчета трафика на основе правил и фильтров
- Межсетевой экран
- Динамическое управление шириной канала
- Блокирования трафика при достижении заданного лимита
- Учет трафика по имени пользователя терминал-сервера или имени процесса
- URL Фильтрация (возможность блокирования WEB-запросов по ключевому слову в адресе, создание «черных» и «белых» списков WEB-сайтов)
- Собственный DNS сервер для обслуживания DNS-запросов пользователей локальной сети
- Собственный DHCP сервер
- Подсчет трафика по протоколу Cisco Netflow
- Клиентский агент авторизации

35.2. Ключевые релизы программы

- июнь 2003 — первый релиз программы.
- 31.08.2004 — версия 5.0. Ядро TMeter работает как Служба Windows.
- 07.09.2006 — версия 6.6. Реализован механизм аутентификации пользователей, что позволило решить проблему подмены IP- и MAC-адресов
- 28.05.2007 — версия 7.5 с встроенным механизмом NAT
- 30.07.2008 — версия 8.1 с собственным DNS-сервером
- 26.01.2009 — версия 9.0. Добавлен механиз URL-фильтрации
- 27.01.2010 — версия 10.0. Добавлена возможность подсчета трафика по имени пользователя терминал-сервера или по имени процесса
- 27.01.2011 — версия 11.0. Добавлен DHCP сервер
- 17.01.2012 — версия 12.0. Добавлена возможность мониторинга хостов путем периодического пингования диапазонов IP-адресов. Результат пингования отображается в виде таблицы со следющими параметрами хоста: статус; IP-адрес; имя в обратной зоне; Mac-адрес; название производителя Mac-адреса; прочий комментарий основанный на IP- или MAC-адресе. Таким образом, вы можете отслеживать появление/исчезание компьютеров в вашей локальной сети (даже если компьютер не отвечает на пинги)

Улучшен алгоритм выхода сервиса из спящего режима Улучшен алгоритм работы шейпера.

- 06.03.2012 — версия 12.1.615. Добавлена поддержка Netflow v.9
- 30.03.2015 — версия 15.0. Полный рефакторинг кода. Добавлено публичное API для службы TMeter.

35.3. Ссылки

- Официальный сайт программы
- Официальный форум программы
- Контроль за трафиком. // computerra, 15 августа 2005 года
- Его Величество Трафик. // computerra, 14 января 2009 года
- TMeter — учет трафика для домашнего пользователя и небольшой офисной сети. // Softkey.info, 04 августа 2008 года

Глава 36

Traffic Inspector

Traffic Inspector — универсальный шлюз безопасности, разрабатываемый российской компанией «Смарт-Софт». Основные задачи программы — организация доступа в Интернет, надежная сетевая защита, отчеты по использованию ресурсов сети Интернет и сертифицированный биллинг.

Traffic Inspector не требует дорогостоящего сетевого оборудования и устанавливается на стандартном персональном компьютере, выполняющем функции шлюза для LAN-сети. Программа поддерживает следующие операционные системы: Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012 и Windows 8.[1]

Traffic Inspector включает набор модулей, расширяющих функциональность программы. Администрирование программы осуществляется в графическом режиме, через оснастку Microsoft Management Console. На сайте разработчика доступна бесплатная 30-дневная пробная версия программы.

36.1. Функиональные возможности

- **Контроль доступа к сети Интернет**. Организация интернет-доступа с разграничениями по пользователям, компьютерам или группам.
- **Сетевая безопасность**. Контекстный межсетевой экран, система предотвращения чрезмерной сетевой активности; антивирусная проверка почтового и веб-трафика на уровне шлюза, фильтрация спама и защита от фишинговых сайтов.
- **Фильтрация веб-трафика**. Запрет доступа к нежелательным веб-сайтам, запрет загрузок нежелательного веб-контента, фильтрация банеров, графики и другого нежелательного медиаконтента.
- **Расширенная маршрутизация**. Поддержка маршрутизации по условию (policy-based routing), резервирование каналов, ограничение скорости работы пользователей (шейпер) и приоритезация трафика, поддержка работы пользователей через NAT и встроенные HTTP/SOCKS-прокси.
- **Биллинг и отчеты**. Система биллинга, учет и тарификация трафика; контроль, статистика, мониторинг сетевой активности пользователей в реальном времени, отчеты по использованию сети Интернет.
- **Интеграция со средой Microsoft Active Directory**. Поддерживается импорт пользователей из доменов Active Directory.
- **Идентификация по SMS**. Процедура, позволяющая однозначно связывать устройство, пытающееся подключиться к Сети с номером телефона конкретного человека.

36.2. Модули

- **Adguard** - фильтрация рекламы, социальных виджетов и всплывающих окон.
- **RAS Dialer** - дозвон и удержание соединений типа Dial-up, VPN, PPPoE.
- **Dr. Web Gateway Security Suite** - антивирусная проверка HTTP и SMTP-трафика, проходящего через прокси-сервер и почтовый шлюз Traffic Inspector .
- **Traffic Inspector Antivirus Powered By Kaspersky** - антивирусная проверка HTTP и SMTP-трафика, проходящего через прокси-сервер и почтовый шлюз Traffic Inspector.
- **Traffic Inspector Anti-Spam Powered By Kaspersky** - фильтр для защиты от спама и нежелательное корреспонденции.
- **NetPolice** - URL-фильтрация и категоризация веб-ресурсов.
- **Fishing Blocker** - защита от фишинговых веб-сайтов.

- **RBL Filter** - фильтрация спама с проверкой email-адресов в он-лайн базах данных.

36.3. Traffic Inspector Enterprise

Traffic Inspector Enterprise – программное обеспечение для централизованного контроля и управления Интернет-доступом и создания доверенной среды для географически распределенной корпоративной сети. Traffic Inspector Enterprise решает следующие задачи:

- Централизованный контроль Интернет-доступа с использованием единой консоли управления
- Сетевая защита региональных офисов с помощью универсального средства противодействия сетевым угрозам
- Возможность головному офису получать отчеты об использовании ресурсов сети Интернет по всем региональным офисам

36.4. Сертификат ФСТЭК

Программа Traffic Inspector имеет в сертификат соответствия № 2407 от 15 августа 2011 года, выданный ФСТЭК РФ. Срок действия сертификата продлен до 15 августа 2017 года.

Сертификат удостоверяет, что программный комплекс Traffic Inspector является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, обрабатываемой в локальных вычислительных сетях с TCP/IP протоколом, соответствует требованиям:

«Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации» - по 3 классу защищенности; «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» - по 4-му уровню контроля.

Сертификат на сайте разработчика

36.5. История обновлений

- май 2003 — первая публикация программы.
- 27.12.2003 — релиз версии 1.0.
- 17.04.2005 — выпущен релиз версии 1.1.3. Реализован шейпер, Advanced Routing, контроль сетевой активности.
- 21.06.2006 — версия 1.1.4 с антивирусной проверкой трафика.
- 17.07.2006 — программа сертифицирована в МинСвязи.
- 27.08.2008 — реализована проверка трафика модулем Касперского
- 28.07.2009 — вышел Traffic Inspector 2.0. Получил новый сертификат связи.
- 21.08.2009 — выпущен модуль защиты от спама.
- 01.08.2010 — выпущен аппаратный аналог программы — интернет-шлюза AquaInspector.
- 25.10.2010 — выпущена версия 2.0.0.636. Новая версия SQLite для встроеной базы данных и усовершенствованный механизм блокировок.
- 03.11.2010 — выпущена версия 2.0.0.637. Реализованы поддержка классификации контента путем присвоения категории интернет-ресурсам и плагин классификации контента.
- 15.08.2011 — программа сертифицирована в ФСТЭК РФ.
- 15.11.2011 — выпущена версия 2.0.1.719. Добавлена синхронизация правил публикации со службой RRAS и ICS. Автоматическое создание пользователей и правил сетевого экрана при публикации. Публикация диапазона портов в одно действие. Поиск сервера по имени в сети.
- 13.12.2011 — добавлен новый бесплатный антифишинговый модуль Phishing Blocker. Модуль разработан на основе технологий API Google Safe Browsing. Он предназначен для защиты от фишинговых сайтов.
- 05.06.2012 - выпущена версия 2.0.1.724. В состав дистрибутива Traffic Inspector добавлен релиз-кандидат антивирусного модуля Dr.Web Gateway Security Suite. Реализовано автоматическое назначение лицензий в модулях.
- 22.08.2012 - выпущена версия 2.0.1.727. Новый драйвер NDIS6 rev. 184. Скрытие предупреждений на главной странице. Отправка запроса на восстановление ключа активации из интерфейса программы.
- 25.09.2012 - версия Traffic Inspector 2.0.1.726. получила сертификат соответствия ФСТЭК К1 №2407.
- 10.10.2012 - версия Traffic Inspector 2.0.1.728 успешно прошла тестирование в компании Microsoft и получила официальные статусы «Совместимо с Windows 8» и «Сертифицировано для Windows Server 2012».

- 15.10.2012 - новый модуль контекстной фильтрации NetPolice интегрирован в программу. Разработанный совместно с ЦАИР, модуль позволяет соблюдать требование Федерального закона № 436 о защите детей от информации, причиняющей вред их здоровью и развитию, который вступил в силу с 1 сентября 2012 года.
- 20.11.2012 - выпущена версия 2.01.729. Релиз модуля Net Police. Возможность импорта пользователей из Active Directory.
- 07.02.2013 - версия 2.01.731. Возможность блокировки и автоматического обновления списков запрещенных ресурсов Интернета согласно ФЗ № 139.
- 10.07.2013 - релиз Traffic Inspector 3.0.0. Новое: Новый интерфейс. Поддержка .Net Framework 4.0. Журнал действий администратора. Поддержка фильтра u32 для анализа трафика (глубокая инспекция пакетов). Возможность отслеживания пользовательских запросов в поисковых системах (Bing, Google, Mail.ru, Rambler, Yahoo, Yandex).
- 18.10.2013 - релиз Traffic Inspector 3.0.1. Основное нововведение версии – служба Traffic Inspector стала 64-х битной. Как результат увеличилось количество пользователей, которые смогут одновременно работать через прокси-сервер Traffic Inspector.
- 14.05.2014 - релиз Traffic Inspector 3.0.1.822 с новым антиспам-модулем Traffic Inspector Anti-Spam powered by Kaspersky.
- 11.07.2014 - получен сертификат ФСТЭК РФ на версию Traffic Inspector 3.0. Кроме того, действие сертификата продлено до 15 августа 2017 года.
- 10.11.2014 - релиз Traffic Inspector 3.0.2.902. Новое: новый web-портал и оптимизированная система отчетов, новый механизм добавления пользователей в программу, функциональность отображения причин блокировки по списку Россвязьнадзора, загрузка компонентов для модулей программы по требованию, отображение заблокированных web-ресурсов в мониторе работы, новый вид административных прав для просмотра отчетов, отображение заблокированных web-ресурсов в мониторе работы.
- 20.01.2015 - релиз Traffic Inspector 3.0.2.903. В новой версии программы реализована функциональность разделения и архивирования баз данных. Администратор просто указывает подходящий интервал создания баз данных. По мере того, как программа переходит на запись в новую базу данных, предыдущие базы можно свободно перенести на другие носители для освобождения места на диске. Создаваемые базы имеют оптимальный размер, что важно для их обслуживания и быстрого построения отчетов. Генерирование отчетов возможно как по текущей базе данных, так и по архивированным базам.
- 27.04.2015 - релиз Traffic Inspector 3.0.2.904. В новой версии программы добавлена поддержка тарифных опций. С помощью тарифных опций провайдер может продавать, а пользователь - приобретать различного рода улучшения для своего тарифного плана. В настоящее время Traffic Inspector поддерживает следующие опции: увеличение скорости работы в Интернете, получение дополнительного объема трафика и безлимитный доступ.
- 31.08.2015 - релиз Traffic Inspector 3.0.2.906. Доработки и изменения: добавлена возможность SMS идентификации пользователей, поддержка ОС Microsoft Windows 10, запись в отчёты информации об активации тарифных опций, добавлен шейпер в тарифную опцию "Безлимитный доступ", добавлена возможность импорта настроек NetPolice для Traffic Inspector и проверки HTTPS контента по категориям через NetPolice для Traffic Inspector, незначительные доработки программного кода. Исправлены ошибки загрузки файлов с некоторых FTP серверов через прокси-сервер Traffic Inspector, несоответствие дат в отчётах при значениях "по умолчанию" одним суткам.

36.6. Ссылки

- Официальный сайт программы
- Официальный форум программы
- Тема по Traffic Inspector на форуме Ru-Board
- Михаил Брод. Чтобы, подсчитав, не прослезиться. // computerra, 29 августа 2005 года
- Шлюз в инет // Хакер, номер № 076 (,,,)
- Алексей Гуров. Сетевой инспектор. // Hi-tech №1 2008
- Михаил Абрамзон. Сетевые инспекторы. Windows в офисе. Что может быть проще? // Журнал "Системный администратор". № 7-8 2011
- Михаил Брод. Контроль и защита трафика// Онлайновый журнал “SoftKey.info”. 2013

Глава 37

Uncomplicated Firewall

Uncomplicated Firewall (ufw) (англ. *незамысловатый межсетевой экран*) — это утилита для конфигурирования межсетевого экрана iptables. Она использует интерфейс командной строки, состоящий из небольшого числа простых команд.

37.1. GUI for Uncomplicated Firewall

GUI for Uncomplicated Firewall (Gufw) (англ. графический интерфейс пользователя для незамысловатого межсетевого экрана) — это, как следует из его названия, графический интерфейс для UFW (Uncomplicated Firewall). Он был разработан для Ubuntu.

UFW предназначен для легкого, интуитивно понятного управления межсетевым экраном Ubuntu. Он поддерживает общие задачи, такие как разрешение или блокирование предварительно настроенных, общих P2P, или отдельных портов. Gufw работает на UFW, запускается на Ubuntu, а также на любой платформе, где доступны Python, GTK+ и UFW.

37.2. Особенности

37.3. Ссылки

- Сайт Gufw (англ.)
- ufw документация на русском языке
- Gufw документация на русском языке

Глава 38

Zentyal

Zentyal (ранее — **eBox Platform**) — это дистрибутив основанный на Ubuntu, с пакетом серверного программного обеспечения с открытым исходным кодом, ориентированный на малые и средние корпоративные сети. Zentyal может выступать в роли сетевого шлюза, единого центра безопасности сети, Office Server, сервера унифицированных коммуникаций или комбинировать любые из перечисленных функций. Кроме того, Zentyal включает фреймворк, упрощающий разработку новых служб для Unix.

Исходный код проекта доступен на условиях лицензии GNU General Public License, а также (частично) под различными проприетарными соглашениями. Zentyal является собственностью и спонсируется испанской коммерческой компанией eBox Technologies S.L., которая владеет авторскими правами на кодовую базу.

38.1. Возможности

По состоянию на июль 2012 актуальной являлась версия Zentyal 2.2.2, обладающая следующими возможностями:[2]

- Организация локальных сетей
  - Сетевой фильтр и роутер
    - Фильтрация
    - NAT и перенаправление портов
    - VLAN 802.1Q
    - поддержка нескольких шлюзов PPPoE и DHCP
    - Правила для нескольких шлюзов, балансировка нагрузки и автоматический перехват управления при отказе
    - Распределение трафика (shaping), в том числе на уровне приложений
    - Мониторинг трафика с графическими отчётами
    - Механизм детектирования вторжений в сеть
    - Клиент Dynamic DNS
  - Сетевая инфраструктура
    - DHCP-сервер
    - NTP-сервер
    - DNS-сервер
      - Динамические обновления через DHCP
    - Сервер RADIUS
  - Поддержка VPN
    - Автоматическая конфигурация динамических правил роутинга
  - HTTP-прокси
    - Интернет-кэш
    - Пользовательская аутентификация
    - Фильтрация контента (со списками категорий)
    - Прозрачная антивирусная проверка
    - Delay pools
  - Система детектирования вторжений
  - Почтовый сервер
    - Виртуальные домены
    - Квоты
    - Поддержка SIEVE
    - Восстановление внешних аккаунтов
    - POP3 и IMAP с SSL/TLS
    - Фильтрация спама и антивирусная проверка
      - грейлистинг, черные и белые списки адресатов
    - Прозрачный фильтр POP3-прокси
    - Аккаунт Catch-all
- Webmail
- Web-сервер
  - Виртуальные хосты
- Авторизация на основе сертификатов
- Рабочие группы
  - Централизованное управление пользователями и группами

    - Поддержка иерархии (Master/slave)
    - Синхронизация с Windows Active Directory
  - Windows PDC
    - Политики паролей
    - Поддержка клиентов на базе Windows 7
  - Общий доступ к сетевым ресурсам
    - Файл-сервер
      - Антивирус
      - Корзина
    - Print-сервер
  - Groupware: календарь, адресная книга, webmail, wiki и др.
  - VoIP-сервер
    - Голосовая почта
    - Комнаты для конференций
    - Звонки через внешнего провайдера
    - Трансферные звонки
    - Удержание звонков
    - Музыка при удержании
    - Квоты
    - Логи
- Сервер Jabber/XMPP
  - Комнаты конференций
- Zentyal User Corner for self users info updating
- Отчёты и мониторинг
  - Панель управления (Dashboard) для централизованного доступа к сервисной информации
  - Мониторинг CPU, загрузки, дискового пространства, температуры, памяти
  - Использование дисков и состояние RAID
  - Полный отчёт по состоянию системы
  - Отправка уведомлений администратору по электронной почте, через RSS или Jabber
- Обновления программного обеспечения
- Резервное копирование (включая конфигурацию и удалённые/remote данные)

38.2. Разработка

Zentyal использует модель open source и его код полностью доступен всем его пользователям.

38.2.1. Архитектура

Zentyal это web-приложение, использующее сервер Apache с mod perl в качестве основы и компоненты Mason для отдельных модулей. Интерфейсная часть также использует Javascript.

38.2.2. Компоненты с открытым исходным кодом

Zentyal собран из отдельных компонентов с открытым исходным кодом, большей частью написанных на Perl:

- Apache web server
- mod perl CGI engine
- OpenLDAP shared users and groups
- OpenSSL cryptography
- netfilter/iptables firewall and NAT
- BIND DNS server
- Squid proxy server and web cache
- DansGuardian content-control software
- Postfix mail transfer agent
- XMPP instant messaging
- ntpd clock synchronization
- OpenVPN VPN
- Samba shared storage and PDC for Windows clients
- CUPS shared printers
- APT software installation and upgrade
- Asterisk VOIP services
- Snort network intrusion detection system
- Zarafa or eGroupWare calendar sharing, address book, and webmail
- Dovecot IMAP and POP3 server

38.3. Сообщество

Основное сообщество Zentyal поддерживается на форуме Zentyal.

38.4. См. также

- ClearOS
- Webmin
- Control panel
- SysCP
- SME Server
- Ajenti

38.5. Примечания

[1] Zentyal announces Zentyal Server 4.0, major new Linux Small Business Server release

[2] Zentyal 2.0 Features. Проверено 1 сентября 2010. Архивировано из первоисточника 1 сентября 2012.

38.6. Ссылки

- Project website
- Developer's website

Глава 39

ZoneAlarm

ZoneAlarm — межсетевой экран, первоначально разработанный Zone Labs, которая была приобретена в марте 2004 года Check Point Software Technologies. Ранее ZoneAlarm был известен как Zone Labs, но использование этого названия сейчас сокращается.

39.1. Возможности программы

Firewall — Проактивная защита от входящих, выходящих и программных нападений, оставаясь невидимым для хакеров.

- Inbound & Outbound — отслеживание и блокирование интернет-угроз.
- Full Stealth Mode — режим полной невидимости (одним из инструментов невидимости является запрет на ICMP-эхо-ответ).
- Kill Controls — мгновенное отключение вредоносных программ.

Anti-Spyware — позволяет автоматически предотвращать, блокировать, и удалять шпионское программное обеспечение.

- Spy Site Blocking — предотвращает случайные посещения и вредоносные передачи со шпионских сайтов.
- Kernel-Level Spyware Prevention — защита на уровне операционной системы.
- Hourly Signature Updates — почасовые обновления.
- Inbound and Outbound MailSafe — проверка подозрительных вложений к почтовым сообщениям.

Total ID Theft Protection — предотвращение краж личных данных.

- PC-Based ID Protection — блокирует, удаляет или отключает программы, предназначенные для кражи личных данных.

Root & Boot Protection — защита операционной системы от руткитов и других атак.

- Operating System Firewall (OSFirewall ™) — постоянная защита от вирусов и программ-шпионов, руткитов, а также от угроз ядру.
- Early Boot Protection — защита операционной системы при запуске.

Additional Layers — интеграция нескольких слоёв современной защиты для повышения безопасности.

- Wireless PC Protection — защита компьютера подключённого к беспроводной сети.
- Privacy Protection — управление и блокировка всплывающих окон, куки, а также кэш-памятью.
- SmartDefense Service — обеспечивает в реальном времени обновления безопасности и более быстрое реагирование на угрозы.

39.2. Версии

- **ZoneAlarm:** Бесплатная версия брандмауэра, включающая в себя веб-экран и сетевой экран с контролем за исходящими соединениями программ и скрытием портов.
- **ZoneAlarm Pro:** Содержит идентичный операционной системе брандмауэр, блокиратор выплывающих окон, модуль детектирования рекламного ПО, блокиратор cookie. Не имеет функции антивируса.
- **ZoneAlarm Anti-Spyware:** Включает в себя все возможности ZoneAlarm Pro, а также защиту конфиденциальных данных от кражи.
- **ZoneAlarm Antivirus:** Включает в себя ZoneAlarm Firewall и антивирусную защиту от Kaspersky Labs.

- **ZoneAlarm Internet Security Suite:** Включает в себя все вышеперечисленные функции, а также экран служб обмена мгновенными сообщениями и антиспам фильтр от MailFrontier и родительский контроль.
- **ZoneAlarm Force Field:** Система виртуализации, защищающая компьютер и персональную информацию от компьютерных интернет-угроз. Включает в себя несколько степеней защиты от фишинга, шпионского ПО и загрузки опасных файлов.
- **ZoneAlarm Extreme Security:** Максимальная версия, включающая в себя все вышеописанные возможности, а также ForceField, систему оптимизации работы компьютера и средство резервного копирования.
- **IMSecure:** Защищает персональные данные пользователя, шифрует переписку, предотвращает другие угрозы от программ обмена мгновенными сообщениями: (AIM, Yahoo!, MSN, ICQ, Trillian).

Разработка следующих версий прекращена:

- **ZoneAlarm Plus:** Разработка прекращена в конце 2004 года. Причина: меньше возможностей, по сравнению с ZoneAlarm Pro, но примерно одинаковая цена.
- **ZoneAlarm Wireless Security:** Разработка прекращена 19 октября 2005, т.к. функциональность этой программы была включена в all paid versions of ZoneAlarm from version 6 onwards.

39.3. Позиции в рейтингах программ класса «Firewall»

На сайте **matousec.com**, посвящённом проблемам защиты персонального компьютера программами класса Firewall, ZoneAlarm Extreme Security 2012 10.0.250.000 занял 11 место в общем зачёте с результатом 72 % и оценкой « Good». Не рекомендован к применению.[1]

39.4. Примечания

[1] Proactive Security Challenge (англ.)

39.5. Ссылки

- Официальный сайт программы

Глава 40

Брандмауэр Windows

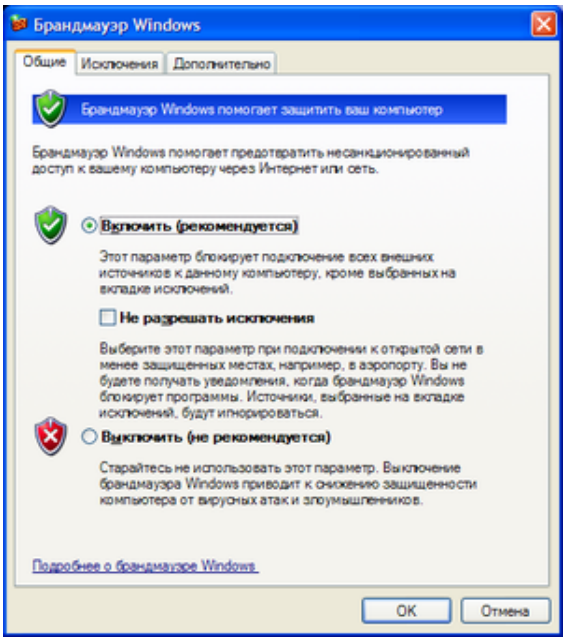
Брандма́уэр Windows — встроенный в Microsoft Windows межсетевой экран. Появился в Windows XP SP2. Одним из отличий от предшественника (Internet Connection Firewall) является контроль доступа программ в сеть. Брандмауэр Windows является частью Центра обеспечения безопасности Windows.

40.1. Обзор

Первоначально Windows XP включала Internet Connection Firewall, который (по умолчанию) был выключен из-за проблем совместимости. Настройки Internet Connection Firewall находились в конфигурации сети, поэтому многие пользователи не находили их. В результате в середине 2003 года компьютерный червь Blaster атаковал большое число компьютеров под управлением Windows, используя уязвимость в службе Удалённый вызов процедур. Через несколько месяцев червь Sasser провёл аналогичную атаку. В 2004 году продолжалось распространение этих червей, в результате чего непропатченные машины заражались в течение нескольких минут[1]. Microsoft подверглась критике, и поэтому решила значительно улучшить интерфейс и функциональность Internet Connection Firewall и переименовать его в «Брандмауэр Windows».

В брандмауэр Windows встроен журнал безопасности, который позволяет фиксировать IP-адреса и другие данные, относящиеся к соединениям в домашних и офисной сетях или в Интернете. Можно записывать как успешные подключения, так и пропущенные пакеты. Это позволяет отслеживать, когда компьютер в сети подключается, например, к web-сайту. Данная возможность по умолчанию отключена (её может включить системный администратор)[2].

40.2. Версии



Брандмауэр Windows под Windows XP Service Pack 2

40.2.1. Windows XP

Брандмауэр Windows был выпущен в составе Windows XP Service Pack 2. Все типы сетевых подключений, такие, как проводное, беспроводное, VPN и даже FireWire, по умолчанию фильтруются через брандмауэр (с некоторыми встроенными исключениями, разрешающими соединения для машин из локальной сети). Это устраняет проблему, когда правило фильтрации применяется лишь через несколько секунд после открытия соединения, создавая тем самым уязвимость[3]. Системные администраторы могут настраивать фаервол, используя групповую политику. Брандмауэр Windows XP не работает с исходящими соединениями (фильтрует только входящие подключения).

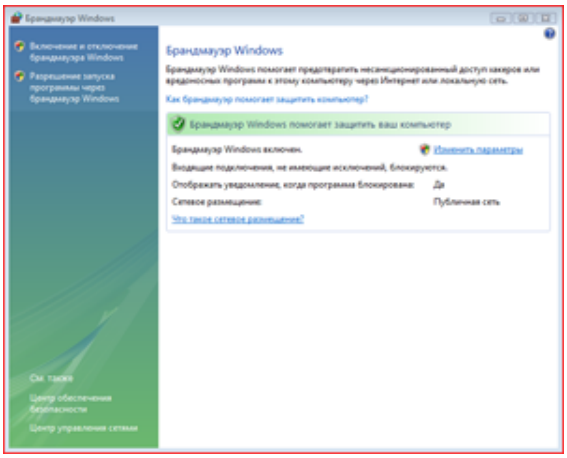
Включение Брандмауэра Windows в SP2 — одна из причин (другой причиной стал DCOM activation security)[4], по которой многие корпорации своевременно не приступили к развёртыванию Service Pack 2. Во время выхода SP2 некоторые web-сайты сооб-

щили о проблемах совместимости со многими приложениями (большинство из которых решаются добавлением исключений в брандмауэр).

40.2.2. Windows Server 2003

В марте 2005 года Microsoft выпустила Windows Server 2003 Service Pack 1, включающий несколько улучшений в брандмауэр данной серверной операционной системы.

40.2.3. Windows Vista



Брандмауэр Windows под Windows Vista

Windows Vista добавляет в брандмауэр новые возможности, улучшающие его развёртывание в корпоративной среде[5]:

- Новая оснастка консоли *Брандмауэр Windows в режиме повышенной безопасности*, позволяющая получить доступ к дополнительным возможностям, а также поддерживающая удалённое администрирование. Получить к ней доступ можно через *Пуск → Панель управления → Администрирование → Брандмауэр Windows в режиме повышенной безопасности* или набрав команду wf.msc.
- Фильтр соединений IPv6.
- Фильтрация исходящего трафика, позволяющая бороться с вирусами и шпионским ПО. Настроить фильтрацию можно, используя консоль управления MMC.
- Используя расширенный фильтр пакетов, правила можно применять к определённым диапазонам IP-адресов и портов.
- Правила для служб можно задавать, используя имена служб из списка, без необходимости указывать полное имя службы.
- Полностью интегрирован IPsec, позволяя фильтровать соединения, основанные на сертификатах безопасности, аутентификации Kerberos и т. п. Шифрование можно требовать для любого типа соединения.
- Улучшено управление сетевыми профилями (возможность создавать разные правила для домашних, рабочих и публичных сетей). Поддержка создания правил, обеспечивающих соблюдение политики изоляции домена и сервера.

40.2.4. Windows Server 2008

Windows Server 2008 содержит брандмауэр, аналогичный версии под Windows Vista.

40.3. См. также

- Сравнение брандмауэров
- Windows Vista
- Список компонентов Windows
- Межсетевой экран
- Microsoft Internet Security and Acceleration Server
- Comodo Firewall Pro

40.4. Заметки

1. ↑ Эти уязвимости были устранены Microsoft в течение нескольких месяцев; подробнее см. бюллетени Microsoft по безопасности MS03-026, MS03-039, и MS04-012.

40.5. Примечания

[1] Study: Unpatched PCs compromised in 20 minutes | CNET News.com

[2] Журнал безопасности брандмауэра подключения к Интернету

[3] The Cable Guy — February 2004

[4] Security-Related Policy Settings

[5] The Cable Guy — January 2006

40.6. Ссылки

- Understanding Windows Firewall (англ.)
- Customizing Windows Firewall (англ.)
- Adding Windows Firewall Exceptions (англ.)
- Working with Windows Firewall API using VC++ (Examples) (англ.)

Глава 41

Интернет Контроль Сервер

Интернет Контроль Сервер — интернет-шлюз на базе операционной системы *FreeBSD*. Основные функции программы — защита корпоративной сети, учёта трафика, управление доступом, сетевые сервисы: почтовый, Web, FTP, Jabber-серверы, IP-телефония, контент-фильтр и др.

41.1. Особенности программы

Коробка программы ИКС

Интернет Контроль Сервер получил 19 апреля 2012 года сертификат ФСТЭК № 2623.

41.2. Награды

- Один из лучших программных продуктов 2011 года по версии русского издания журнала PCmagazine[1]
- Награда Approved by Anti-Malware.ru 2012 г.
- Лауреат премии PC Magazine/RE BestSoft 2013
- Интернет Контроль Сервер получил премию Best Soft 2014

41.3. Примечание

[1] pcmag.ru/reviews/sub_detail.php?ID=45662&SUB_PAGE=0 Лучшие программные продукты — 2011

41.4. Ссылки

- Описание функциональных возможностей программы Интернет Контроль Сервер
- http://www.pcmag.ru/columns/detail.php?ID=45489 — Алексей Гуськов, «А-Реал Консалтинг» (рус.). PC Magazine/RE (2011-11-02). Проверено 27 апреля 2012.

Статья Межсетевой экран ИКС поддерживает высокие стандарты безопасности]

- http://www.pcmag.ru/columns/detail.php?ID=47328 — Игорь Алексеев, исполнительный директор «А-Реал Консалтинг» (рус.). PC Magazine/RE (2012-10-12). Проверено 12 декабря 2012.
- http://pcmag.ru/library/detail.php?ID=47766 — Техническое описание программы Интернет Контроль Сервер (рус.). PC Magazine/RE (2013-02-05). Проверено 10 февраля 2013.
- Anti-Malware.ru — Обзор Интернет Контроль Сервер (ИКС) 2.3.4 ФСТЭК

Глава 42

Интернет-шлюз

Интернет-шлюз — как правило, это программное обеспечение, призванное организовать передачу трафика между разными сетями. Программа является рабочим инструментом системного администратора, позволяя ему контролировать трафик и действия сотрудников.

42.1. Описание

Обычно Интернет-шлюз позволяет распределять доступ среди пользователей, вести учёт трафика, ограничивать доступ отдельным пользователям или группам пользователей к ресурсам в Интернет. Интернет-шлюз может содержать в себе прокси-сервер, межсетевой экран, почтовый сервер, шейпер, антивирус и другие сетевые утилиты. Интернет-шлюз может работать как на одном из компьютеров сети, так и на отдельном сервере. Шлюз устанавливается как программное обеспечение на машину с операционной системой, либо на пустой компьютер с развертыванием встроенной операционной системы.

Также под шлюзом часто понимается IP-адрес машины, через которую организован доступ в интернет.

42.2. См. также

- Сетевой шлюз
- Шлюз по умолчанию
- Маршрутизатор

42.3. Ссылки

- Выбираем корпоративный интернет-шлюз

Глава 43

Континент (программа)

АПКШ «Континент» (аппаратно-программный комплекс шифрования «Континент») — аппаратно-программный комплекс, позволяющий обеспечить защиту информационных сетей организации от вторжения со стороны сетей передачи данных (Интернет), конфиденциальность при передаче информации по открытым каналам связи (VPN), организовать безопасный доступ пользователей VPN к ресурсам сетей общего пользования, а также защищенное взаимодействие сетей различных организаций[1][2].

Программа объединяет межсетевой экран и средство построения VPN-сетей. Является сертифицированным продуктом и обладает сертификатами ФСТЭК и ФСБ. Изначально разработана компанией НИП «Информзащита», далее разработка выделена в ООО "Код Безопасности".

Аппаратно-программный комплекс шифрования «Континент» широко используется государственными структурами России[3], например Казначейством Российской федерации[4].

43.1. Назначение

Программа предназначена для объединения через Интернет локальных сетей предприятия в единую сеть VPN. Поддерживает подключение удалённых и мобильных пользователей к VPN по защищённому каналу, разделение доступа между информационными подсистемами организации, безопасное удалённое управление маршрутизаторами. Может использоваться для организации защищённого взаимодействия со сторонними организациями.

Является одной из немногих российских сертифицированных программ с высокой производительностью (в режиме VPN — 800 Мбит/сек)[5]. Входит в число наиболее популярных VPN-продуктов в России[6].

Программа, например, используется в таком крупном общероссийском проекте, как СУФД — Система удаленного финансового документооборота или СУФД-онлайн.
Федеральное казначейство России в рамках реализации проекта «Модернизации казначейской системы Российской Федерации» планирует перевести своих клиентов с ППО СЭД на СУФД-онлайн до конца 2013 года.[7][8][9][10]

43.2. Недостатки

- До версии 3.6 не работает за NAT, из-за использования нестандартного протокола IP 250.
- Отсутствие CLI-интерфейса.
- Низкий уровень поддержки Unix-систем.
- До версии 3.7 Отсутствие поддержки синхронизации времени NTP.
- Отсутствие настройки времени в GUI управления.
- До версии 3.7 Отсутствие возможности назначать статические адреса для клиентов СД.
- Высокая цена.

43.3. Примечания

[1] Континент-К. Аппаратно-программный комплекс. cnews.ru. Проверено 10 ноября 2012. Архивировано из первоисточника 21 ноября 2012.

[2] *Корнюшин П.Н., Костерин А.С.* Информационная безопасность: Учебное пособие * Единое окно доступа к образовательным ресурсам.. window.edu.ru (2003). Проверено 10 ноября 2012. Архивировано из первоисточника 21 ноября 2012.

[3] CNews: АПКШ «Континент» пропустили в госсектор. cnews.ru. Проверено 10 ноября 2012. Архивировано из первоисточника 21 ноября 2012.

[4] Управление Федерального казначейства по Республике Калмыкия. kalmykia.roskazna.ru. Проверено 10 ноября 2012. Архивировано из первоисточника 21 ноября 2012.

[5] ФЗ−152 в здравоохранении: как «обезопасить» ЛПУ?. cnews.ru. Проверено 10 ноября 2012. Архивировано из первоисточника 21 ноября 2012.

[6] Интернет-издание о высоких технологиях. cnews.ru. Проверено 10 ноября 2012. Архивировано из первоисточника 21 ноября 2012.

[7] Управление Федерального казначейства по г. Санкт-Петербург

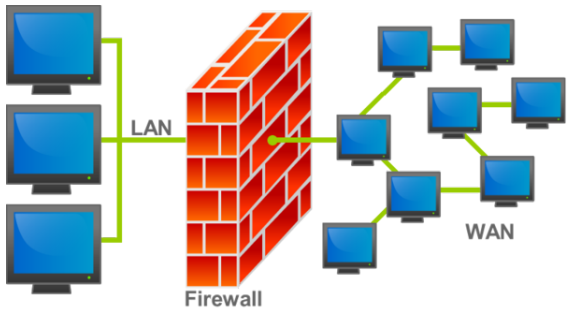
[8] СУФД-онлайн - Главная

[9] Сайт технической поддержки пользователей ПО (СУФД, СУФД Онлайн, Портал АРМ ДУБП, АСФК, АРМ Генерации ключей, Континент АП, скачать)

[10] Арх-СУФД-Портал

Глава 44

Межсетевой экран



Иллюстрация, показывающая расположение межсетевого экрана в сети.

Межсетево́й экра́н, **сетево́й экра́н** — это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита сети или отдельных её узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых (серых) адресов или портов на внешние, используемые за пределами локальной сети, — что может обеспечивать дополнительную безопасность.

44.1. Другие названия

Брандма́уэр (нем. *Brandmauer*) — заимствованный из немецкого языка термин, являющийся аналогом английского *firewall* в его оригинальном значении (противопожарная перегородка — стена, которая разделяет смежные здания, предохраняя от распространения пожара). Интересно, что в области компьютерных технологий в немецком языке употребляется слово *Firewall*.

Файрво́лл, **файрво́л**, **файерво́л**, **фаерво́л** — образовано транскрипцией английского термина *firewall*.

44.2. Разновидности сетевых экранов

Поддерживаемый уровень сетевой модели OSI является основной характеристикой при классификации межсетевых экранов. Различают следующие типы межсетевых экранов:

1. Управляемые коммутаторы (канальный уровень).
2. Сетевые фильтры сетевого уровня (stateless). Фильтрация статическая, осуществляется путём анализа IP-адреса источника и приёмника, протокола, портов отправителя и получателя.
3. Шлюзы сеансового уровня (circuit-level proxy). В сетевой модели TCP/IP нет уровня, однозначно соответствующего сеансовому уровню OSI, поэтому к шлюзам сеансового уровня относят фильтры, которые невозможно отождествить ни с сетевым, ни с транспортным, ни с прикладным уровнем:
   - Шлюзы, транслирующие адреса (NAT, PAT) или сетевые протоколы (транслирующий мост);
   - Фильтры контроля состояния канала. К фильтрам контроля состояния канала связи нередко относят сетевые фильтры сетевого уровня с расширенными возможностями (stateful), которые дополнительно анализируют заголовки пакетов и умеют фильтровать фрагментированные пакеты);
   - Шлюзы сеансового уровня. Наиболее известным и популярным шлюзом сеансового уровня является посредник SOCKS;
4. Шлюз прикладного уровня (application-level proxy), часто называемые прокси-серверами.

Делятся на прозрачные (transparent) и непрозрачные (solid).

5. Брандмауэр SPI (Stateful Packet Inspection, SPI), или иначе брандмауэры с динамической фильтрацией пакетов (Dynamic Packet Filtering), являются по сути шлюзами сеансового уровня с расширенными возможностями. Инспекторы состояния оперируют на сеансовом уровне, но «понимают» протоколы прикладного и сетевого уровней. В отличие от шлюза прикладного уровня, открывающего два виртуальных канала TCP (один — для клиента, другой — для сервера) для каждого соединения, инспектор состояния не препятствует организации прямого соединения между клиентом и сервером.

Существует также понятие «межсетевой экран экспертного уровня». Сетевой экран данного типа базируются на посредниках прикладного уровня или инспекторах состояния, но обязательно комплектуются шлюзами сеансового уровня и сетевыми фильтрами, иногда понимая и сетевой уровень. Зачастую имеют систему протоколирования событий и оповещения администраторов, средства поддержки удаленных пользователей (например авторизация), средства построения виртуальных частных сетей и т. д. К нему относятся почти все имеющиеся на рынке брандмауэры.

44.3. Типичные возможности

- фильтрация доступа к заведомо незащищенным службам;
- препятствование получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
- контроль доступа к узлам сети;
- может регистрировать все попытки доступа как извне, так и из внутренней сети, что позволяет вести учёт использования доступа в Интернет отдельными узлами сети;
- регламентирование порядка доступа к сети;
- уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран;

Вследствие защитных ограничений могут быть заблокированы некоторые необходимые пользователю службы, такие как Telnet, FTP, SMB, NFS, и так далее. Поэтому настройка файрвола требует участия специалиста по сетевой безопасности. В противном случае вред от неправильного конфигурирования может превысить пользу.

Также следует отметить, что использование файрвола увеличивает время отклика и снижает пропускную способность, поскольку фильтрация происходит не мгновенно.

44.4. Проблемы, не решаемые файрволом

Межсетевой экран сам по себе не панацея от всех угроз для сети. В частности, он:

- не защищает узлы сети от проникновения через «люки» (англ. *back doors*) или уязвимости ПО;
- не обеспечивает защиту от многих внутренних угроз, в первую очередь — утечки данных;
- не защищает от загрузки пользователями вредоносных программ, в том числе вирусов;

Для решения последних двух проблем используются соответствующие дополнительные средства, в частности, антивирусы. Обычно они подключаются к файрволу и пропускают через себя соответствующую часть сетевого трафика, работая как прозрачный для прочих сетевых узлов прокси, или же получают с файрвола копию всех пересылаемых данных. Однако такой анализ требует значительных аппаратных ресурсов, поэтому обычно проводится на каждом узле сети самостоятельно.

44.5. Литература

- *Дэвид В. Чепмен, мл., Энди Фокс.* Брандмауэры Cisco Secure PIX = Cisco® Secure PIX® Firewalls. — М.: «Вильямс», 2003. — С. 384. — ISBN 1-58705-035-8.

44.6. См. также

- Маршрутизатор
- Персональный файрвол
- Великий китайский файрвол
- Интернет-шлюз
- Демилитаризованная зона (DMZ)

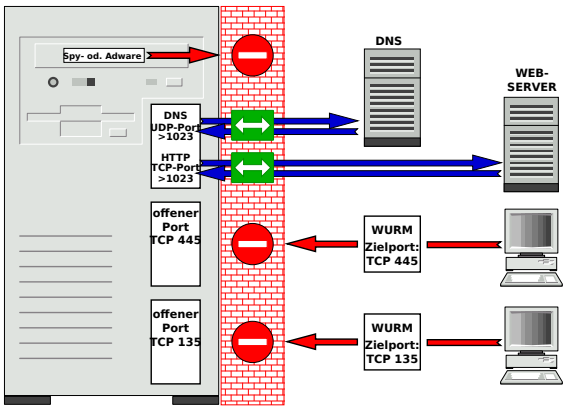
44.7. Примечания

44.8. Ссылки

- Лекция 10 «Межсетевые экраны» / Эрик Мэйволд, Безопасность сетей: Информация, ИНТУИТ 2006, ISBN 978-5-9570-0046-9
- Шлюзы безопасности: новая волна / «Журнал сетевых решений/LAN», № 09, 2010

Глава 45

Персональный файрвол



Персональный файрвол[1] (также *персональный брандмауэр*) — программное обеспечение, осуществляющее контроль сетевой активности компьютера, на котором он установлен, а также фильтрацию трафика в соответствии с заданными правилами. В отличие от межсетевого экрана, персональный файрвол устанавливается непосредственно на защищаемом компьютере.

Функционал персонального файрвола подобен функциональности межсетевого экрана, однако, в силу своей специфики, персональный файрвол так же может обеспечивать дополнительные возможности для защиты компьютера:

- Контроль за приложениями, использующими порты. Персональный файрвол, в отличие от обычных межсетевых экранов, способен определить не только используемый протокол и сетевые адреса, но программное обеспечение, устанавливающее или принимающее сетевое соединение.
- Назначение раздельных правил разным пользователям без дополнительной сетевой авторизации.
- Специальный «Режим обучения», необходимый для тонкой настройки персонально файрвола под конкретную программную конфигурацию компьютера. В данном режиме при первичной сетевой активности любого программного обеспечения пользователь получает запрос на разрешение или запрещение сетевой активности данного приложения.

Несмотря на наличие некоторых полезных функций, выгодно отличающих персональный файрвол от межсетевого экрана, следует понимать, что персональный файрвол не предназначен для использования в качестве межсетевого экрана и не может осуществлять фильтрацию маршрутизируемых и/или транслируемых пакетов.

45.1. См. также

- Межсетевой экран

45.2. Примечания

[1] «ФАЙРВОЛ(Л): рекоменд. *файрвол*, не рекоменд. *файервол(л)*, *файэрвол(л)*» // *И. Мостицкий.* Универсальный дополнительный практический толковый словарь. — 2012.

Глава 46

Сетевой шлюз

Сетевой шлюз со встроенным коммутатором. Вид спереди (вверху) и сзади (внизу)

Сетевой шлюз (англ. *gateway*) — аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).

46.1. Описание

Сетевой шлюз конвертирует протоколы одного типа физической среды в протоколы другой физической среды (сети). Например, при соединении локального компьютера с сетью Интернет обычно используется сетевой шлюз.

Маршрутизатор (он же — роутер) является одним из примеров аппаратных сетевых шлюзов.

Сетевые шлюзы работают на всех известных операционных системах. Основная задача сетевого шлюза — конвертировать протокол между сетями. Роутер сам по себе принимает, проводит и отправляет пакеты только среди сетей, использующих одинаковые протоколы. Сетевой шлюз может с одной стороны принять пакет, сформатированный под один протокол (например Apple Talk) и конвертировать в пакет другого протокола (например TCP/IP) перед отправкой в другой сегмент сети. Сетевые шлюзы могут быть аппаратным решением, программным обеспечением или тем и другим вместе, но обычно это программное обеспечение, установленное на роутер или компьютер. Сетевой шлюз должен понимать все протоколы, используемые роутером. Обычно сетевые шлюзы работают медленнее, чем сетевые мосты, коммутаторы и обычные маршрутизаторы. Сетевой шлюз — это точка сети, которая служит выходом в другую сеть. В сети Интернет узлом или конечной точкой может быть или сетевой шлюз, или хост. Интернет-пользователи и компьютеры, которые доставляют веб-страницы пользователям — это хосты, а узлы между различными сетями — это сетевые шлюзы. Например, сервер, контролирующий трафик между локальной сетью компании и сетью Интернет — это сетевой шлюз.

В крупных сетях сервер, работающий как сетевой шлюз, обычно интегрирован с прокси-сервером и межсетевым экраном. Сетевой шлюз часто объединен с роутером, который управляет распределением и конвертацией пакетов в сети.

Сетевой шлюз может быть специальным аппаратным роутером или программным обеспечением, установленным на обычный сервер или персональный компьютер. Большинство компьютерных операционных систем использует термины, описанные выше. Компьютеры под Windows обычно используют встроенный мастер подключения к сети, который по указанным параметрам сам устанавливает соединение с локальной или глобальной сетью. Такие системы могут также использовать DHCP-протокол. Dynamic Host Configuration Protocol (DHCP) — это протокол, который обычно используется сетевым оборудованием, чтобы получить различные данные, необходимые клиенту для работы с протоколом IP. С использованием этого протокола добавление новых устройств и сетей становится простым и практически автоматическим.

46.2. См. также

- Интернет-шлюз

46.3. Ссылки

- Сетевые технологии. Средства межсетевого обмена (рус.)

Глава 47

Антивирусная программа

Антиви́русная програ́мма (антиви́рус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

47.1. Целевые платформы антивирусного ПО

На данный момент антивирусное программное обеспечение разрабатывается, в основном, для ОС семейства Windows от компании Microsoft. Это вызвано большим количеством вредоносных программ именно под эту платформу (а это, в свою очередь, вызвано большой популярностью этой ОС, так же, как и большим количеством средств разработки, в том числе бесплатных и даже «инструкций по написанию вирусов»). В настоящий момент на рынок выходят продукты и для других операционных систем, таких, к примеру, как Linux и Mac OS X. Это вызвано началом распространения компьютерных вирусов и под эти платформы, хотя UNIX-подобные системы традиционно пользуются репутацией более устойчивых к воздействию вредоносных программ.

Помимо ОС для настольных компьютеров и ноутбуков, также существуют платформы и для мобильных устройств, такие, как Windows Mobile, Symbian, Apple iOS, BlackBerry, Android, Windows Phone 7 и др. Пользователи устройств на данных ОС также подвержены риску заражения вредоносным программным обеспечением, поэтому некоторые разработчики антивирусных программ выпускают продукты и для таких устройств.

47.2. Классификация антивирусных продуктов

По используемым технологиям антивирусной защиты:

- Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования, продукты, применяющие только проактивные технологии антивирусной защиты);
- Комбинированные продукты (продукты, применяющие как сигнатурные методы защиты, так и проактивные)

По функционалу продуктов:

- Антивирусные продукты (продукты, обеспечивающие только антивирусную защиту)
- Комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции)

По целевым платформам:

- Антивирусные продукты для ОС семейства Windows
- Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.)
- Антивирусные продукты для ОС семейства MacOS
- Антивирусные продукты для мобильных платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone 7 и др.)

Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:

- Антивирусные продукты для защиты рабочих станций
- Антивирусные продукты для защиты файловых и терминальных серверов
- Антивирусные продукты для защиты почтовых и Интернет-шлюзов
- Антивирусные продукты для защиты серверов виртуализации
- и т.д.

47.3. Антивирусы для сайтов

Их можно поделить условно на несколько типов:

- Серверный — устанавливается на веб-сервер. Поиск вирусов, в этом случае, происходит в файлах всего сервера.
- Скрипт или компонент CMS — выполняющие поиск вредоносного кода, непосредственно в файлах сайта.
- SaaS сервис — система централизованного управления, позволяющая управлять файлами, базами данных, настройками и компонентами веб-ресурсов на VDS и DS удаленно.

47.4. Специальные антивирусы

В ноябре 2014 года международная правозащитная организация Amnesty International выпустила антивирусную программу Detect, предназначенную для выявления вредоносного ПО, распространяемого государственными учреждениями для слежки за гражданскими активистами и политическими оппонентами. Антивирус выполняет более глубокое сканирование жёсткого диска, нежели обычные антивирусы[1][2].

47.5. Лжеантивирусы

В 2009 началось активное распространение лжеантивирусов — программного обеспечения, не являющегося антивирусным (то есть не имеющего реальной функциональности для противодействия вредоносным программам), но выдающим себя за таковое. По сути, лжеантивирусы могут являться как программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением. В настоящий момент это распространение приостановлено.

47.6. Работа антивируса

Говоря о системах Майкрософт, следует знать, что обычно антивирус действует по схеме:

- поиск в базе данных антивирусного ПО сигнатур вирусов.
- если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс «карантина», и процесс блокируется.
- зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.

47.7. Базы антивирусов

Для использования антивирусов необходимы постоянные обновления так называемых баз антивирусов. Они представляют собой информацию о вирусах — как их найти и обезвредить. Поскольку вирусы пишут часто, то необходим постоянный мониторинг активности вирусов в сети. Для этого существуют специальные сети, которые собирают соответствующую информацию. После сбора этой информации производится анализ вредоносности вируса, анализируется его код, поведение, и после этого устанавливаются способы борьбы с ним. Чаще всего вирусы запускаются вместе с операционной системой. В таком случае можно просто удалить строки запуска вируса из реестра, и на этом в простом случае процесс может закончиться. Более сложные вирусы используют возможность заражения файлов. Например, известны случаи, как некие даже антивирусные программы, будучи зараженными, сами становились причиной заражения других чистых программ и файлов. Поэтому более современные антивирусы имеют возможность защиты своих файлов от изменения и проверяют их на целостность по специальному алгоритму. Таким образом, вирусы усложнились, как и усложнились способы борьбы с ними. Сейчас можно увидеть вирусы, которые занимают уже не десятки килобайт, а сотни, а порой могут быть и размером в пару мегабайт. Обычно такие вирусы пишут в языках программирования более высокого уровня, поэтому их легче остановить. Но по-прежнему существует угроза от вирусов, написанных на низкоуровневых машинных кодах наподобие ассемблера. Сложные вирусы заражают операционную систему, после чего она становится уязвимой и нерабочей.

47.8. Примечания

[1] AI разработала программу, которая спасет журналистов от киберслежки

[2] BBC:«How to stop governments spying on you»

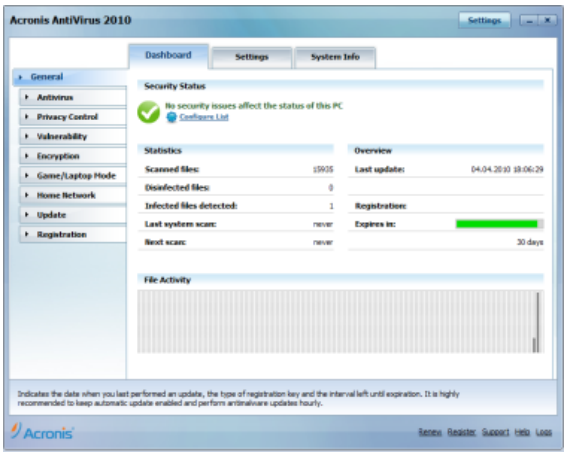
Глава 48

Acronis AntiVirus

Acronis AntiVirus — антивирусная программа, выпускаемая компанией Acronis. Антивирус основан на движке BitDefender[2].

48.1. Функционал

Версия интерфейса для новичков



Версия интерфейса для экспертов

Антивирус включает в себя[3]:

- Антивирус;
- анти-фишинг;
- анти-руткит;
- шифрование IM-трафика;

Также в антивирусе можно выбрать три уровня сложности интерфейса в зависимости от уровня подготовки пользователя[3]. В продукт встроен «игровой режим»[3].

48.2. Распространение

Стоимость Acronis AntiVirus составляет $39,99 за годовую лицензию на 3 компьютера[3] (около $13 за один компьютер). Поддержка русского языка пока отсутствует.

48.3. Примечания

[1] Backup software for data backup and disaster recovery in Windows and Linux — Acronis

[2] Acronis AntiVirus 2010: Trojan.FakeAlert.5 on Windows x64 Systems | Knowledge Base

[3] Acronis Antivirus 2010 features: scan and remove viruses and spyware from your PC, IM encryption, Rootkit elimination

48.4. Ссылки

- Официальный сайт

Глава 49

ActiveVirusShield

ActiveVirusShield — бесплатный антивирусный продукт AOL на базе Антивируса Касперского 6.

Программа включает в себя:

- Резидентный файловый монитор (сканер по доступу);
- Компонент, защищающий электронную почту получаемую по протоколам POP3, IMAP4 и отправляемую по протоколу SMTP;
- Антивирусный сканер с возможностью сканирования по расписанию и с заданием предопределённых задач сканирования (критические объекты, объекты автозапуска), а также возможность создавать свои собственные задачи.

Созданный на основе Антивируса Касперского 6, он отличается от него оформлением, наличием (пока) только англоязычной версии и отсутствием некоторых компонентов:

- Проактивная защита;
- Защита интернет соединений.

Антивирус бесплатный для загрузки для всех пользователей (членство в AOL не требуется), для работы необходим лицензионный номер, высылаемый на адрес электронной почты.

Последние версии антивируса поддерживают 32- и 64-битные версии MS Windows Vista.

Начиная с августа 2007 года возможность получать активационные ключи и скачать дистрибутив с сайта AOL закрыта, вместо AVS подписчикам AOL предлагается скачать и установить McAfee Virus Scan Plus — специальное издание от AOL, также доступного им платно.[1]

49.1. Примечания

[1] AOL Security Central: McAfee VirusScan Plus — Special Edition from AOL — Discover AOL

49.2. Ссылки

- Официальный сайт
- Сайт поддержки

Глава 50

Advanced SystemCare

Advanced SystemCare – это программа, которая обеспечивает автоматический сервис для ПК с удалением вредоносных программ, исправлением ошибок в реестре, защитой личных данных, очисткой системы и повышением производительности. Присутствуют модули по защите настроек браузера,ускорение доступа при пользовании Интернетом, а также защиту от вирусов, но не может заменить полноценный антивирус.

50.1. Функции

- Базовая защита от компьютерных угроз, блокирование несанкционированного доступа к личным данным
- Базовая оптимизация системы
- Защита при скачивании и совместном использовании файлов
- Оптимизация в режиме реального времени с Active Boost
- Очистка системного реестра
- Более 20 средств для оптимизации работы компьютера
- ВНИМАНИЕ! Высокий шанс лишиться Windows! Слетает после полного ухода. (ver. 8 PRO)

50.2. Ссылки

- Обзор Advanced SystemCare от Softkey (англ.)
- Описание работы программы Advanced SystemCare от Softkey (англ.)
- О выпуске обновленной утилиты Advanced SystemCare от club.cnews.ru (англ.)
- О выпуске обновленной утилиты Advanced SystemCare от softodrom.ru (англ.)
- Описание программы от comss.ru (англ.)
- Описание программы от softportal.com (англ.)
- IObit Advanced SystemCare 4 – тюнинг и оптимизация работы ПК. Ferra.ru (англ.)

Глава 51

Advanced SystemCare Ultimate

Advanced SystemCare Ultimate — это программное обеспечение, которое интегрирует антивирус, оптимизацию ПК и работу в интернете в единое решение. Программа предотвращает зависания и фатальные сбои без снижения производительности системы. Advanced SystemCare Ultimate можно использовать совместно с другими защитными программами.

51.1. Принцип работы

Advanced SystemCare Ultimate сочетает в себе технологии антивируса BitDefender и собственный защитный механизм фирмы IObit[1].

51.2. Функции

51.2.1. Защита

- Анализ особенностей информационной безопасности Windows
- Обнаружение и удаление шпионских программ и рекламных модулей
- Защита при загрузке и совместном использовании файлов
- Безопасное пользование Интернетом
- Защита без снижения производительности системы

51.2.2. Производительность

- Повышение производительности компьютера за счет оптимизации Windows
- Повышение скорости работы в Интернет за счет высвобождения собственной мощности системы с Internet Booster
- Оптимизация в режиме реального времени с Active Boost (Технология Active Boost непрерывно работает в фоновом режиме и обнаруживает неиспользуемые ресурсы)
- Глубокая очистка системного реестра
- Максимальная производительность жесткого диска
- Более 20 «умных» средств для улучшения работы компьютера
- Возможность переключаться между режимом для работы и режимом для игр

51.2.3. Защита личных данных

- Автоматическое удаление конфиденциальных данных
- Блокирование несанкционированного доступа к личным данным

51.3. Критика

Некоторые пользователи критикуют программу за то, что она выполняет «фиктивные» действия. Например, находит вирусы и трояны после собственной же очистки системы. По лёгкости установки программа получила одну звезду из 5, так как из 12 тестовых систем корректно она была установлена только на 11[2].

51.4. Примечания

[1] Advanced SystemCare Ultimate 6 - новая программа для обеспечения безопасности ПК (рус.). Проверено 20 января 2015.

[2] Advanced SystemCare Ultimate 6 (англ.). Проверено 20 января 2015.

51.5. Ссылки

- Advanced SystemCare Ultimate (с Антивирусом) // comss.ru
- Advanced SystemCare Ultimate с Антивирусом 8.0.1.660 // soft.softodrom.ru
- Advanced SystemCare Ultimate 8.0.1.660 (англ.) // softpedia.com
- Advanced SystemCare Ultimate 6 — новая программа для обеспечения безопасности ПК // IXBT.com
- Advanced SystemCare Ultimate 6 (англ.) // pcmag.com

Глава 52

Aidstest

«Aidstest» — антивирусная программа-сканер (полифаг). Предназначена для поиска и обезвреживания файловых, загрузочных и файлово-загрузочных вирусов. Поиск вирусов Aidstest осуществляет с помощью сигнатур. Поддерживалась и распространялась на протяжении 1988—1998 годов ЗАО «ДиалогНаука». На зарубежных рынках распространялась под названием V-Hunter (Virus Hunter) и имела версии на английском и немецком языках. Автор программы — Дмитрий Лозинский.

52.1. История

Первая советская программа-антивирус. Создана в 1988 году, когда один из компьютеров Главного вычислительного центра Госплана СССР оказался заражён вирусом Vienna-648[1]. В своё время — один из известнейших[2] в СССР и России отечественных программных продуктов.

В конце 90-х Aidstest был заменён Doctor Web'ом. Основной причиной прекращения работы над Aidstest было широкое распространение в то время полиморфных вирусов, полностью изменяющих свой код при каждом заражении. Так как в подобных вирусах нельзя было выделить постоянную сигнатуру, Aidstest априори не мог с ними бороться, в то время как антивирус Doctor Web, также поддерживаемый ЗАО «ДиалогНаука», справлялся с этой задачей. Это привело к тому, что развитие Aidstest было признано бесперспективным, а его создатель подключился к разработке антивируса Doctor Web.

52.2. Примечания

[1] *Гриднева Н.* Человек, который поймал вирус (рус.) // Коммерсантъ-Деньги : журнал. — М., 10 апреля 1996. — № 13 (73). — С. 5.

[2] *Быковский Е.* Вирус уничтожен (рус.) // Итоги : журнал. — М., 1999. — № 46.

52.3. Ссылки

- Интернет-архив, сохраненная копия сайта "Диалог-Наука", октябрь 1996 г.

Глава 53

Ashampoo AntiSpyWare

Ashampoo AntiSpyWare — антивирусное программное обеспечение, разрабатываемое германской частной компанией Ashampoo. Предоставляет пользователю защиту от вирусов, троянских, шпионских программ, руткитов и adware.

53.1. Описание

Антишпионское решение от компании Ashampoo, предназначенное для защиты и отражению опасных и подозрительных объектов исходящих из Интернета.

Обладает приличным набором инструментов от вирусов, шпионов, перехватчиков клавиатурного ввода, рекламных модулей и прочих опасных программ, которые могут нарушить работоспособность компьютера или украсть личные данные.

В базе данных Ashampoo AntiSpyWare хранится около 2 009 156 вредоносных объектов, программа способна мониторить системную деятельность в фоновом режиме, благодаря постоянному активному сканеру, предоставляя защиту, а также пути решения в реальном времени на компьютере, не мешая работе пользователя.

Используя эвристическое сканирование установленное в настройках, способна проверить абсолютно все файлы в системе, к примеру, архивы защищённые паролем, опознавать неизвестные сигнатуры или потоковые данные в файловой системе NTFS, а также отталкивать те подозрительные и вредосносные программы, которые ещё неизвестны.

Антивирус не является кроссплатформенным программным обеспечением и работает только на компьютерах под управлением операционной системы Microsoft Windows.

53.2. Возможности

Включает в себя различные режимы сканирования и осуществляет проверку:

-
  - всего компьютера.
  - указанную пользователем область.
  - системных областей.
  - жёстких дисков.
  - на наличие руткитов.
  - системного реестра.
  - cookies браузеров.
  - определенных папок.
- Надежный блокировщик рекламы, которая поступает через популярные программы (Windows Media Player, MSN Messenger, QuickTime и прочих).
- Детектор Rootkit (может работать без вмешательства Ashampoo AntiSpyWare и запускаться пользователем отдельно).
- Интернет очистка (удаление всех следов вебсёрфинга в сети).
- Компактный и простой в использовании графический интерфейс.
- Карантинная зона.
- Менеджер автозапуска.
- Журнал событий.
- Планировщик заданий.
- Также в стандартную комплектацию входят дополнительные инструменты для обеспечения безопасности.
  - *File Wiper*. Безвозвратное уничтожение файлов, папок или целых дисков.
  - *Hosts File Checker*. Поверка файла хостов Windows на перенаправления и их удаление, в случае необходимости.
  - *StartUp Tuner*. Проверка и определение приложений, которые должны загружаться при запуске Windows.

- *Rootkit Detector*. Сканирование системы на наличие скрытых процессов и файлов.
- *Internet Checker*. Удаление файлов кэша, cookies и истории известных браузеров.
- *ADS Scanner*. Поиск на NTFS дисках дополнительных потоков, которые невидны в проводнике и их удаление, в случае необходимости.
- *Process manager*. Просмотр информации о процессах и их завершение, если необходимо.
- *LSP Viewer*. Управление установленными WinSock LSP, которые влияют на поведение сети и Интернета.

53.3. Ссылки

- Страница программы Ashampoo AntiSpyWare (англ.)
- Безопасность: Ashampoo AntiSpyWare v.2.05. iXBT (20 января 2009). Проверено 13 августа 2010. Архивировано из первоисточника 6 мая 2012.

Глава 54

Ashampoo AntiVirus

Ashampoo AntiVirus — антивирусное программное обеспечение, разрабатываемое германской частной компанией Ashampoo. Предоставляет пользователю защиту от вирусов, троянских и шпионских программ, руткитов, Adware с ежедневным обновлением своих баз данных.

54.1. Описание

Является очень маленьким по размеру, а также экономным в потреблении системных ресурсов. Благодаря встроенной проактивной защите способен обнаруживать вирусы, которые отсутствуют в базе данных. Также антивирус можно настроить так чтобы он обнаруживал какие-то вирусные игры[*неизвестный термин*], сайты и другое.

Включает в себя различные режимы и осуществляет проверку:

- всего компьютера.
- памяти.
- системных областей.
- жёстких дисков.
- CD/DVD.
- папок

Ко всему прочему, программа оснащена антивирусным монитором, планировщиком заданий, карантинной областью и журналом событий. Может интегрироваться в оболочку Windows и производить сканирование выбранных папок/файлов из контекстного меню, а также, при установленной опции, выключить компьютер по завершению проверки объектов на наличие вредоносных программ.

Антивирус не является кроссплатформенным программным обеспечением и работает только на компьютерах под управлением операционной системы Microsoft Windows.

54.2. Ссылки

- Страница программы Ashampoo AntiVirus (англ.)
- Антивирусы: Ashampoo AntiVirus v.1.50. iXBT (1 сентября 2007). Проверено 10 августа 2010. Архивировано из первоисточника 6 мая 2012.
- *Сергей и Марина Бондаренко.* Ashampoo AntiVirus 1.30: антивирус для вашего ПК. 3DNews (25 декабря 2006). Проверено 10 августа 2010.

Глава 55

AVZ

AVZ — бесплатная антивирусная программа.

Помимо стандартных сканеров (с эвристическим анализатором) и ревизора включает в себя ряд средств автоматизации удаления вредоносного кода, часть из которых являются нетипичными (на 2007 год) и предоставляют достаточно грамотному пользователю расширенные средства контроля.

Программа была разработана Олегом Зайцевым. С 2007 года Олег работает[2] в Лаборатории Касперского и остаётся единственным разработчиком AVZ. Используемые в AVZ наработки и технологии вошли в основные продукты Лаборатории Касперского — Kaspersky Internet Security 2009/2010 и Kaspersky for Windows Workstations 6 MP4.

55.1. Назначение

Программа служит для нахождения и удаления:

- Spyware и Adware
- Троянских программ
- Backdoor
- Вирусов
- Сетевых червей
- Почтовых червей
- Руткитов
- Кейлогеров

Программу также применяют для создания логов, полезных при запросе помощи на антивирусных форумах.

55.2. Средства, встроенные в AVZ[3]

Микропрограммы эвристической проверки систем Микропрограммы проводят поиск известных spyware и вирусов по косвенным признакам — на основании анализа реестра, файлов на диске и в памяти.

Обновляемая база безопасных файлов В неё входят цифровые подписи десятков тысяч системных файлов и файлов известных безопасных процессов. База подключена ко всем системам AVZ и работает по принципу «свой/чужой» — безопасные файлы не вносятся в карантин, для них заблокировано удаление и вывод предупреждений, база используется антируткитом, системой поиска файлов, различными анализаторами. В частности, встроенный диспетчер процессов выделяет безопасные процессы и сервисы цветом, поиск файлов на диске может исключать из поиска известные файлы (что очень полезно при поиске на диске троянских программ).

Детектор руткитов (встроенный) Поиск руткитов идёт без применения сигнатур, на основании исследования базовых системных библиотек на предмет перехвата их функций. AVZ может не только обнаруживать руткиты, но и производить корректную блокировку работы руткитов. Противодействие руткитам распространяется на все сервисные функции AVZ, в результате сканер AVZ может обнаруживать маскируемые процессы, система поиска в реестре «видит» маскируемые ключи и т. п. Антируткит снабжён анализатором, который проводит обнаружение процессов и сервисов, маскируемых руткитами. Особенностью системы противодействия руткитам является её работоспособность в Windows 9x. Другой особенностью является универсальная система обнаружения и блокирования KernelMode руткитов, работоспособная под Windows NT, Windows 2000 pro/server, XP, XP SP1, XP SP2, XP SP3, Windows 2003 Server, Windows 2003 Server SP1.

Детектор клавиатурных шпионов и троянских DLL Поиск кейлогеров и троянских DLL ведётся на

основании анализа системы без применения базы сигнатур, что может позволить детектировать заранее неизвестные троянские DLL и кейлогеры, но также возможны и ложные срабатывания .

Нейроанализатор Помимо сигнатурного анализатора, AVZ содержит нейроэмулятор, который позволяет производить исследование подозрительных файлов при помощи нейронной сети. В настоящее время нейросеть применяется в детекторе кейлогеров.

Анализатор Winsock SPI/LSP настроек (встроенный)
Позволяет проанализировать настройки, диагностировать возможные ошибки в настройке и произвести автоматическое лечение. Возможность автоматической диагностики и лечения полезна для начинающих пользователей (в утилитах типа LSPFix автоматическое лечение отсутствует). Для исследования SPI/LSP вручную в программе имеется специальный менеджер настроек LSP/SPI. На работу анализатора Winsock SPI/LSP распространяется действие антируткита.

Диспетчер процессов, сервисов и драйверов (встроенный)
Предназначен для изучения запущенных процессов и загруженных библиотек, запущенных сервисов и драйверов. На работу диспетчера процессов распространяется действие антируткита (как следствие — он «видит» маскируемые руткитом процессы). Диспетчер процессов связан с базой безопасных файлов AVZ, опознанные безопасные и системные файлы выделяются цветом.

Утилита для поиска файлов на диске (встроенная)
Позволяет искать файл по различным критериям, возможности системы поиска превосходят возможности системного поиска. На работу системы поиска распространяется действие антируткита (как следствие — поиск «видит» маскируемые руткитом файлы и может удалить их), фильтр позволяет исключать из результатов поиска файлы, опознанные AVZ как безопасные. Результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно пометить группу файлов для последующего удаления или помещения в карантин.

Утилита для поиска данных в реестре (встроенная)
Позволяет искать ключи и параметры по заданному образцу, результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно отметить несколько ключей для их экспорта или удаления. На работу системы поиска распространяется действие антируткита (как следствие — поиск «видит» маскируемые руткитом ключи реестра и может удалить их).

Анализатор открытых портов TCP/UDP (встроенный)
На него распространяется действие антируткита, в Windows XP для каждого порта отображается использующий порт процесс. Анализатор опирается на обновляемую базу портов известных троянских/Backdoor программ и известных системных сервисов. Поиск портов троянских программ включён в основной алгоритм проверки системы — при обнаружении подозрительных портов в протокол выводятся предупреждения с указанием, каким троянских программам свойственно использование данного порта.

Анализатор общих ресурсов, сетевых сеансов и открытых по сети файлов (встроенный)
Работает в Windows 9x и в NT/2k/XP.

Анализатор Downloaded Program Files (DPF) (встроенный)
Отображает элементы DPF, подключён ко всем системам AVZ.

Микропрограммы восстановления системы
Микропрограммы проводят восстановления настроек Internet Explorer, параметров запуска программ и иные системные параметры, повреждаемые вредоносными программами. Восстановление запускается вручную, восстанавливаемые параметры указываются пользователем.

Эвристическое удаление файлов Суть его состоит в том, что если в ходе лечения удалялись вредоносные файлы и включена эта опция, то производится автоматическое исследование системы, охватывающее классы, BHO, расширения IE и Проводника, все доступные AVZ виды автозапуска, Winlogon, SPI/LSP и т. п. Все найденные ссылки на удалённый файл автоматически вычищаются с занесением в протокол информации о том, что конкретно и где было вычищено. Для этой чистки активно применяется движок микропрограмм лечения системы.

Проверка архивов Начиная с версии 3.60, AVZ поддерживает проверку архивов и составных файлов. На настоящий момент проверяются архивы формата ZIP, RAR, CAB, gzip, tar; письма электронной почты и MHT-файлы; CHM-архивы.

Проверка и лечение потоков NTFS Проверка NTFS-потоков включена в AVZ начиная с версии 3.75.

Скрипты управления Позволяют администратору написать скрипт, выполняющий на ПК пользователя набор заданных операций. Скрипты позволяют применять AVZ в корпоративной сети, включая его запуск в ходе загрузки системы.

Анализатор процессов Анализатор использует нейросети и микропрограммы анализа, он включается при включении расширенного анализа на максимальном уровне эвристики и предназначен для поиска подозрительных процессов в памяти.

Система AVZGuard Предназначена для борьбы с трудноудалимыми вредоносными программами, может кроме AVZ защищать указанные пользователем приложения, например, другие антишпионские и антивирусные программы.

Система прямого доступа к диску для работы с заблокированными файлами
Работает на FAT16/FAT32/NTFS, поддерживается на всех операционных системах линейки NT, позволяет сканеру анализировать заблокированные файлы и помещать их в карантин.

Драйвер мониторинга процессов и драйверов AVZPM
Предназначен для отслеживания запуска и остановки процессов и загрузки/выгрузки драйверов для поиска маскирующихся драйверов и обнаружения искажений в описывающих процессы и драйверы структурах, создаваемых DKOM-руткитами.

Драйвер Boot Cleaner Предназначен для выполнения чистки системы (удаление файлов, драйверов и служб, ключей реестра) из KernelMode. Операция чистки может выполняться как в процессе перезагрузки компьютера, так и в ходе лечения.

55.3. Примечания

[1] Download / Скачать

[2] Новость на сайте. Архивировано из первоисточника 5 июня 2012.

[3] Назначение программы и решаемые ею задачи

55.4. Ссылки

- Интервью с создателем
- AVZ перешёл к Касперским
- Раздел поддержки утилиты на форуме ЛК

Глава 56

BitDefender

BitDefender — румынская компания BitDefender SRL, разрабатывающая и выпускающая антивирусы, файрволы и антиспамовые решения под маркой BitDefender. Данные программы используются более чем в 100 странах мира, и являются особо популярными в Германии и Франции. Согласно официальному сайту, насчитывается около 500 миллионов индивидуальных и корпоративных пользователей.

Компания предлагает свои решения самому широкому кругу клиентов. Программные продукты компании доступны для различных операционных систем, включая Microsoft Windows, различные дистрибутивы Linux и FreeBSD. А также мобильных устройств на базе iOS и Android — как для пользователей, так и для корпоративной защиты BYOD.

На 2015 год компания занимает 1-е место по числу проданных лицензий на антивирусную технологию. Её антивирусный движок (как основной или в дополнение к другим) используют такие компании как Arcabit, Ashampoo, Auslogics, Avetix, BullGuard, CharityAntivirus ApS, Chili Security, Emsisoft, MicroWorld Technologies, MYSecurityCenter, ESTsoft, F-Secure, G Data Software, Hauri, IObit, Lavasoft, Norman, nProtect, Optenet, Qihoo 360 Technology, Roboscan, SurfRight, TrustPort, Wontok[1][*неавторитетный источник? 268 дней*].

56.1. Программные продукты

BitDefender Total Security

BitDefender Total Security включает: антивирус и антишпион, антифишинг, файрвол BitDefender, антиспам BitDefender, родительский контроль.

BitDefender Internet Security

Это решение для рабочих станций, включающее антивирус, файрвол, защиту против спама и программ-шпионов (spyware), а также механизмы родительского контроля.

BitDefender Antivirus Plus (ранее — BitDefender Professional Plus)

Подобен BitDefender Internet Security и включает антивирус, антиспамовую защиту и файрвол. Однако модуль файрвол имеет менее гибкие настройки, а также в нём отсутствуют механизмы родительского контроля.

BitDefender AntiSpyware

BitDefender AntiSpyware — средство антишпионской (antispyware) защиты, которая не включает никаких способностей антивируса. Функциональные возможности этой программы встроены в модуль антивируса, который включается во все другие продуктами BitDefender (кроме BitDefender Free Edition и BitDefender Linux Edition).

BitDefender Free Edition

Бесплатная версия антивируса BitDefender представляет собой предыдущую версию антивирусного продукта. Эта версия включает антивирусный монитор, обеспечивающий постоянную защиту от вирусов, а также имеет возможности удалять и обнаруживать программы-шпионы (spyware). Данный продукт разработан для постоянного использования в качестве альтернативы многим платным антивирусам.

BitDefender Scanner для Unix

Программа предназначена для сканирования файлов по запросу и работает под управлением различных версий Linux и FreeBSD, используя тот же антивирусный механизм, что и другие продукты компании.

BitDefender Mail Protection для Unix

Обеспечивает защиту трафика электронной почты от вирусов, spyware и спама для различных почтовых серверов, работающих под управлением ОС Linux и FreeBSD.

BitDefender для Palm OS

Бесплатный антивирус для карманных компьютеров под управлением Palm OS. BitDefender для Palm OS сканирует все исполняемые файлы во внутренней памяти устройства и представляет отчётную информацию в виде списка, антивирус имеет чёрно-белый интерфейс низкого разрешения, что делает его пригодным для использования на устаревших устройствах.

BitDefender TrafficLight

Бесплатное средство (плагин) для защиты пользователя от веб-угроз.

56.2. Примечания

[1] Антивирусы: Сторонние движки (рус.). Computer Security Software Russia (5 декабря 2014). — «Лидером здесь является Bitdefender, который снабжает своим антивирусным движком большинство решений из представленных в нашем списке» Проверено 5 апреля 2015.

56.3. Ссылки

- Официальный международный сайт компании
- Страница бесплатной версии антивируса BitDefender
- BitDefender GravityZone
- Обзор BitDefender Total Security 2015 на Softkey.ua
- Страница бесплатной версии антивируса для Android

Глава 57

BitDefender TrafficLight

BitDefender TrafficLight — бесплатное приложение для защиты пользователя от веб-угроз, разработанное румынской компанией BitDefender с применением облачных технологий. Продукт распространяется в виде программного решения для Mozilla Firefox, Google Chrome, Safari, а также в виде отдельного расширения для Chromium и браузеров на его основе (Google Chrome, CoolNovo и другие).

57.1. Особенности

BitDefender TrafficLight обладает проактивным анализатором, сканирующим веб-трафик на предмет шпионского ПО и фишинга прежде, чем они достигнут браузера и смогут нанести вред пользователю. При этом, если сайт в целом надёжен, но содержит небезопасные элементы, то защитные модули заблокируют только опасное содержимое[1]. Для большей безопасности программа проводит интеграцию в поисковые системы, такие как Google или Bing, анализируя результаты поисковой выдачи и оценивая их безопасность. Дополнительную функциональность предоставляет сервис сокращения ссылок, который также проверяет надёжность и безопасность ссылок. При этом, как отмечают обозреватели, несомненным плюсом программного решения является его минимализм, так как никакие тулбары не устанавливаются, лишь появляется небольшой индикатор, не отвлекающий от работы[2].

57.2. Примечания

[1] TrafficLight Features (англ.)(недоступная ссылка — *история*). BitDefender (2011 год). — «TrafficLight won't block an entire website if just some pages within are malicious. Only the potentially harmful elements are blocked, leaving you free to view the rest of the site if you so choose.» Проверено 23 марта 2011. Архивировано из первоисточника 20 марта 2011.

[2] *Mike Williams.* Stop malware at the TrafficLight (англ.). Betanews, Inc. (21 марта 2011). — «In fact the only sign TrafficLight is doing anything at all is a tiny traffic light block at the top of the page you're currently displaying» Проверено 23 марта 2011. Архивировано из первоисточника 26 июля 2012.

57.3. См. также

Web of Trust — подобное программное обеспечение, работающее на основе пользовательских оценок.

57.4. Ссылки

Официальные сайты

- TrafficLight Powered by BitDefender (англ.). BitDefender. Проверено 22 марта 2011. Архивировано из первоисточника 13 мая 2012.

Обзоры в прессе

- *Mike Williams.* Block malware, malicious links and more with BitDefender TrafficLight (англ.). Haymarket Media/PC Authority (21 марта 2011 года). Проверено 23 марта 2011. Архивировано из первоисточника 13 мая 2012.
- *Lee Mathews.* BitDefender Traffic Light protects your Web browser from malware and phishing (англ.). DownloadSquad (21 марта 2011 года). Проверено 23 марта 2011. Архивировано из первоисточника 13 мая 2012.
- *Neil J. Rubenking.* BitDefender TrafficLight Enters Beta (англ.). PCMag.com (22 марта 2011). Проверено 24 марта 2011. Архивировано из первоисточника 24 марта 2011.

Глава 58

Bullguard Internet Security

Bullguard Internet Security — антивирусный комплекс от датской компании Bullguard. Программа совмещает в себе антивирус, сетевой экран и утилиту резервного копирования. Bullguard также предоставляет 5 ГБ места на собственном сервере для хранения резервных копий[1]. В качестве антивирусного движка использован таковой от компании BitDefender и файрвол Outpost [2][3][4].

58.1. Состав

Bullguard Internet Security состоит из следующих компонентов[1]:

- антивирус и антишпион на движке BitDefender
- сетевой экран;
- фаервол от Outpost
- антиспам;
- утилита резервного копирования.
- родительский контроль
- оптимизация системы

Также комплекс защищает от фишинга, сканирует трафик IM-программ, таких как MSN, Yahoo и Skype[1]. Антивирус оснащён особым «игровым режимом», при которым потребляется меньше системных ресурсов[1].

58.2. Распространение

Стоимость Bullguard Internet Security составляет $69,95[1]. Для загрузки доступна бесплатная 60-дневная версия[1].

58.3. Примечания

[1] Antivirus Internet Security Package from BullGuard

[2] Outpost firewall

[3] Windows systems downed by dodgy bitdefender update — The Inquirer

[4] How to Install Bullguard | eHow.com

58.4. Ссылки

Официальный сайт (англ.)

Глава 59

CA Antivirus

CA Anti-Virus 8.1 — антивирусное программное обеспечение, разрабатываемое Computer Associates. Предоставляет защиту от вирусов, троянских программ, шпионских программ, а также централизованный механизм обновлений всех объектов антивирусной защиты. Предназначено как для защиты отдельных десктопов, так и для гетерогенных корпоративных сетей с большим количеством серверов и рабочих станций.

Подразделение, занимавшееся разработкой антивируса, в настоящий момент продано компанией Computer Associates. Обозревателями отмечается крайне низкий процент обнаружения угроз и редкий выпуск обновлений[1].

59.1. Достоинства

Приложение CA Anti-Virus упрощает управление угрозами корпоративной безопасности, снижает риск простоя, уменьшает или исключает расходы на восстановление работоспособности системы и на службу поддержки, повышает производительность ИТ-персонала и обеспечивает непрерывность обслуживания.

59.2. Основные возможности

- Пошаговая блокировка вирусов
- Автоматические обновления с эффективным использованием полосы пропускания
- Многоуровневая защита от угроз
- Предупреждения в режиме реального времени
- Гибкие возможности сканирования
- Поддержка Microsoft Vista

59.3. Системные требования

59.3.1. Обычный компьютер

- Процессор Pentium 150 или выше
- 64 Мб свободного дискового пространства
- 512 Мб оперативной памяти
- Windows NT 4.0, SP6A или выше
- Windows 2000
- Windows Server 2003
- Windows XP Professional
- Windows Vista Desktop

59.3.2. Сервер

- Процессор Pentium 4 2.6 ГГц или выше
- 10 Гб свободного дискового пространства
- 1 Гб оперативной памяти
- Windows NT 4.0, SP6A или выше
- Windows 2000 Server
- Windows 2003 Server
- Windows XP Professional
- Windows 2000 Workstation
- Windows Vista OS

59.4. Примечания

[1] CA Internet Security Suite Plus 2008

59.5. Ссылки

- CA antivirus unit sold: Will become 'Total Defense'
- CA Internet Security Suite Plus 2008
- CA Internet Security Suite Plus 2008

Глава 60

Comodo Antivirus

Comodo AntiVirus — бесплатный антивирус с закрытым кодом компании Comodo для Microsoft Windows XP, Vista, Windows 7 и Windows 8. Comodo AntiVirus входит в состав Comodo Internet Security.

60.1. Возможности программы

- Эвристический анализ.
- Проактивная защита.
- Защита от переполнения буфера.
- Встроенный планировщик сканирования.
- Ежедневные, автоматические обновления антивирусных баз.
- Изолирование подозрительных файлов в карантин для предотвращения инфекции.
- Обнаружение, блокирование и удаление вирусов из настольных компьютеров и сетей.

60.2. Особенности программы

Проактивная защита включает в себя HIPS (Host Intrusion Prevention Systems) — система отражения локальных угроз. Задачей HIPS является контроль за работой приложений и блокировка потенциально опасных операций по заданным критериям.

60.3. Примечания

[1] https://forums.comodo.com/news-announcements-feedback-cis/comodo-internet-security-8204674-with-win10-support-is-released-t112353.0.html

[2] https://forums.comodo.com/comodo-antivirus-for-mac-os-x-cavm/comodo-antivirus-for-mac-11214829106-released-t78271.0.html

[3] https://forums.comodo.com/comodo-antivirus-for-linux-cavl/comodo-antivirus-for-linux-cavl-v112680251-is-released-t92199.0.html

60.4. Ссылки

- Сайт компании Комодо (Английский)
- Информация о антивирусных базах
- Русскоязычная часть форума Comodo
- Страница загрузки Comodo AntiVirus
- Сайт компании Comodo: Защита компьютеров под управлением Windows 8 (Английский)
- Гид: пять бесплатных антивирусов (недоступная ссылка с 10-08-2013 (871 день) — *история*, *копия*), «Компьютерра», 22 мая 2007 г
- Ещё раз о бесплатных антивирусах, 3dnews.ru, 13 марта 2007 г

Глава 61

COMODO Cleaning Essentials

Comodo Cleaning Essentials (CCE) — представляет собой набор инструментов компьютерной безопасности, призванный помочь пользователям обнаружить и удалить вредоносные программы и небезопасные процессы с зараженных компьютеров. Состоит из сканера вредоносного кода, а также инструментов Killswitch и Autorun Analyzer. Не требует установки и может работать со сменных носителей, включая USB-флеш-накопитель, CD- или DVD-диск.

61.1. Инструменты

- Сканер вредоносных программ — полностью настраиваемый сканер, который находит и удаляет вирусы, руткиты, скрытые файлы и ключи реестра вредоносных и глубоко скрытых в операционной системе программ. Присутствуют три режима сканирования: «разумное», полное и выборочное.

- Comodo Killswitch (уничтожитель) — инструмент мониторинга системы, который позволяет пользователям идентифицировать, отслеживать и пресекать любые небезопасные процессы, запущенные на их системе. KillSwitch создан на базе программы Process Hacker, но в него добавлены некоторые важные функции, такие как онлайн проверка процессов, уничтожение руткитов и другой замаскированной заразы.

- Comodo Autorun Analyzer (анализатор автозагрузки) — инструмент, позволяющий просматривать, отключать и удалять запускающиеся при старте операционной системы сервисы, приложения и другие компоненты. Позволяет быстро перейти в то место, откуда запускается интересующее приложение/сервис. При необходимости можно скрыть все безопасные элементы автозагрузки, оставив лишь подозрительные (по версии Comodo), затем сформировать запрос о любом приложении/сервисе и отправить его в поисковую систему Google. Данный инструмент является аналогом утилиты AutoRuns.

61.2. Особенности

- Портативный, нет необходимости установки
- Проверяет неопознанные процессы при помощи сервиса Comodo Malware Analysis
- Проверяет MBR на наличие подозрительных модификаций
- Возможность принудительного удаления вредоносных файлов и процессов
- Возможность ведения журнала загрузки системы с помощью KillSwitch

61.3. Примечания

[1] COMODO Cleaning Essentials 2.5.242177.201 released

61.4. Ссылки

- Страница программы на сайте производителя
- ОписаниеComodo Cleaning Essentials на www.comss.ru

Глава 62

Dr. Solomon's Anti-Virus Toolkit

Dr. Solomon's Anti-Virus Toolkit — первая широко известная антивирусная программа, написанная английским программистом Аланом Соломоном (Alan Solomon) в 1988 году. Включала в себя функции предотвращения заражения, обнаружения вирусов, а также восстановление заражённых файлов.

Она завоевала огромную популярность и просуществовала вплоть до 1998 года, когда компания Dr. Solomon была поглощена другим производителем антивирусов — американской Network Associates Inc (NAI).

Выпускалась для платформ Windows (до версии Windows 98 включительно), Novell, Unix, Solaris, и OS/2[1].

62.1. История

Dr. Solomon's Anti-Virus был выпущен 1 марта 1997 и стал конкурировать с лидерами рынка Symantec Norton Anti-Virus и McAfee VirusScan за конечного потребителя.

После некоторой напряжённости в отношениях между двумя вышеназванными программными продуктами,[2] 9 июня 1998 McAfee согласилась приобрести Dr Solomon's Group P.L.C, ведущего европейского производителя антивирусного программного обеспечения, за 642 млн. долларов.[3].

62.2. Примечания

[1] Антивирус Dr. Solomon (англ.) (Проверено 10 октября 2009)

[2] McAfee Versus Dr. Solomon: Fresh Round of Antivirus Mudslinging — статья в журнале PC World от 8 апреля 1997 (англ.) (Проверено 10 октября 2009)

[3] Network Associates Plans to Integrate Dr Solomon's Tools — статья в журнале PC World от 21 августа 1998 (англ.) (Проверено 10 октября 2009)

Глава 63

Dr.Web

Dr.Web (рус. ***Доктор Веб***) — общее название семейства программного антивирусного ПО для различных платформ (Windows, OS X, Linux, мобильные платформы) и линейки программно-аппаратных решений (Dr.Web Office Shield[1]), а также решений для обеспечения безопасности всех узлов корпоративной сети (Dr.Web Enterprise Suite[2]). Разрабатывается компанией «Доктор Веб».

Продукты предоставляют защиту от вирусов, троянского, шпионского и рекламного ПО, червей, руткитов, хакерских утилит, программ-шуток, а также неизвестных угроз с помощью различных технологий реального времени и превентивной защиты.

63.1. Особенности

- Возможность установки на зараженную машину.
- Обнаружение и лечение сложных полиморфных, шифрованных вирусов и руткитов.
- Возможность настройки копирования важных данных в защищённое хранилище позволяет пользователям версии Dr.Web для Windows самостоятельно восстанавливать поврежденные данные без необходимости обращения в службу технической поддержки «Доктор Веб».
- Поддержка большинства существующих форматов упакованных файлов и архивов, в том числе многотомных и самораспаковывающихся архивов.
- Компактная вирусная база и небольшой размер обновлений. Одна запись в вирусной базе позволяет определять до тысячи подобных вирусов.
- Обновления вирусных баз производятся немедленно по мере выявления новых вирусов, до нескольких раз в час. Разработчики антивирусного продукта отказались от выпуска обновлений вирусных баз по какому-либо графику, поскольку вирусные эпидемии не подчиняются таковым.
- Кроссплатформенность — используется единая вирусная база и единое ядро антивирусного сканера на разных платформах ОС.
- Низкое влияние на производительность системы. Благодаря технологиям оптимизации, заведомо чистые файлы не проверяются компонентами Dr.Web, что снижает нагрузку на систему.

63.2. Сравнение функционала защитных решений для Windows

Персональные продукты для Windows разделены на 3 редакции: «**Антивирус Dr.Web**», «**Dr.Web Security Space**» и «**Dr.Web Бастион**». Последние 2 отличаются лишь наличием в комплекте «**Dr.Web Бастион**» криптографа Atlansys Bastion Pro стороннего разработчика — компании «Программные системы Атлансис».

Помимо полноценных антивирусных комплексов, в арсенале компании присутствует продукт под названием «**Dr.Web Katana**», который позиционируется как несигнатурный антивирус для превентивной защиты от новейших активных угроз, целевых атак и попыток проникновения, в том числе через уязвимости «нулевого дня», которые еще не известны антивирусу. «**Dr.Web Katana**» сочетается с уже установленным антивирусом другого производителя.

63.3. Основные продукты

Компания «Доктор Веб» — российская компания, являющаяся производителем и поставщиком антивирусных продуктов под маркой Dr.Web. Компания предлагает антивирусные решения самому широкому кругу клиентов, использующих различные операционные системы.

Основные продукты, разрабатываемые и поставляемые компанией «Доктор Веб»:

- для защиты рабочих станций и файловых серверов под управлением Windows;
- для защиты корпоративной сети и сетей национального масштаба с централизованным управлением антивирусной защитой;
- сервис AV-desk[3] для ISP;
- для защиты почтовых и файловых серверов под UNIX-системами;
- для защиты интернет-шлюзов под UNIX-системами;
- для защиты файловых серверов под Novell NetWare;
- для защиты серверов Lotus Domino на платформе Microsoft Windows;
- для защиты серверов Microsoft Exchange;
- для защиты КПК под управлением Windows Mobile;
- для защиты рабочих станций Mac OS X;
- для защиты смартфонов под управлением Symbian OS;
- для защиты смартфонов и Интернет-планшетов под управлением Android;
- для защиты смартфонов под управлением BlackBerry OS.

63.3.1. Для ОС Windows

Dr.Web Security Space

Полноценный антивирусный комплекс, включающий в себя все последние технологии сигнатурного и несигнатурного детектирования и удаления всех видов вредоносного ПО. Включает антивирус, брандмауэр, веб-антивирус, антиспам, родительский контроль, резервное копирование данных.

История развития версий:

CureIt!

Dr.Web CureIt![9] — утилита для проверки и лечения зараженных рабочих станций на платформе Windows от вредоносного ПО. С версии 8.0 используется универсальная подсистема нейтрализации угроз Anti-rootkit API (ArkAPI), что позволяет лечить систему от вредоносного ПО любой сложности. Оснащен интуитивно понятным интерфейсом, благодаря которому пользователь может в несколько кликов проверить и в случае заражения, вылечить свой ПК. Для опытных же пользователей есть выборочная проверка. Оснащен собственным менеджером карантина, что позволяет восстанавливать резервные копии вылеченных\удаленных файлов даже при повторном запуске утилиты. Используется тот же файловый движок, что и в антивирусе.

Число запусков данной программы не ограничивается. Для обновления антивирусной базы необходимо загрузить с сайта актуальную версию программы (нет возможности автоматического обновления).

С осени 2009 года изменены условия лицензирования сканера — теперь бесплатно использовать его могут только домашние пользователи, использование для организаций и в коммерческих целях стало платным. Кроме того, пользователь бесплатной утилиты обязывается участвовать в программе улучшения качества программного обеспечения, для чего информация, собранная во время проверки компьютера, автоматически отправляется в компанию «Доктор Веб»[10].

CureNet!

Dr.Web CureNet! — сетевая утилита с централизованным управлением для удаленной проверки и лечения зараженных рабочих станций и серверов Windows даже полностью изолированных от Интернета. Позволяет использовать одновременно 2 антивируса на рабочих станциях и файловых серверах Windows: Dr.Web и антивирус другого производителя.

63.3.2. Dr.Web Mobile Security Suite

Это программное обеспечение, предназначенное для комплексной защиты мобильных устройств. В Dr.Web Mobile Security Suite объединены средства защиты для мобильных устройств под управлением Windows Mobile, Symbian OS, BlackBerry OS и Android. Разработчики компании реализовали технологию фильтрации входящих телефонных звонков и СМС-сообщений на основе черного и белого списков. Для платформы Android существует бесплатная версия **Антивирус Dr.Web Light**, в которой нет модуля фильтрации звонков и SMS-сообщений, а также отсутствует компонент «Антивор». На данный момент Антивирус Dr.Web Light занимает 2-е место в топе бесплатных приложений русскоязычного сегмента Android Market, уступая по популярности только программе Skype.[11]

63.4. Уникальные технологии

- **Fly-code** — эмулятор с динамической трансляцией кода, реализующий механизм универсальной распаковки вирусов, защищённых от

анализа и детектирования одним или цепочкой новых и/или неизвестных упаковщиков, крипторов и дропперов. Это позволяет распаковывать файлы, защищенные, к примеру, ASProtect, EXECryptor, VMProtect и тысячами других упаковщиков и протекторов, включая неизвестные антивирусу.

- **Origins Tracing** — алгоритм несигнатурного обнаружения вредоносных объектов, который дополняет традиционные сигнатурный поиск и эвристический анализатор, дает возможность значительно повысить уровень детектирования ранее неизвестных вредоносных программ. Также используется в *Dr.Web для Android*

- **Anti-rootkit API (ArkAPI)** - подсистема, использующая универсальные алгоритмы нейтрализации угроз. Посредством этой системы происходит нейтрализация угроз всеми компонентами антивируса. Так же используется в лечащей утилите Dr.Web CureIt!

- **Dr.Web Shield** — механизм борьбы с руткитами, реализованный в виде драйвера. Обеспечивает низкоуровневый доступ к вирусным объектам, скрывающимся в глубинах операционной системы.

- **SelfPROtect —** модуль самозащиты, защищающий компоненты антивируса (файлы, ключи реестра, процессы и т. д.) от изменения и удаления вредоносным ПО.

- **Background Rootkit Scan** — подсистема фонового сканирования и нейтрализации активных угроз. Данная подсистема находится в памяти в резидентном состоянии и осуществляет сканирование системы на предмет активных угроз и их нейтрализацию в различных областях, например: объекты автозагрузки, запущенные процессы и модули, системные объекты, оперативная память, WMI, MBR/VBR дисков, системный BIOS компьютера.

- **Dr.Web Cloud** — сервис облачной проверки ссылок и файлов на серверах компании «Доктор Веб» в режиме реального времени, позволяющий антивирусу использовать наиболее свежую информацию о небезопасных ресурсах и файлах.

- Dr.Web Process Heuristic (DPH) — технология реального времени, которая защищает от новых, наиболее актуальных вредоносных программ, разработанных с расчетом на необнаружение традиционными сигнатурными и эвристическими механизмами, которые еще не поступили на анализ в антивирусную лабораторию, а значит, неизвестны вирусной базе Dr.Web на момент проникновения в систему.

- Dr.Web Process Dumper (DPD) — технология реального времени, значительно повышает уровень детектирования «новых угроз» — известных вирусной базе Dr.Web, но скрытых под новыми упаковщиками.

- **Dr.Web HyperVisor** — компонент, запускающийся и работающий ниже уровня операционной системы, что обеспечивает контроль всех программ, процессов и работы самой ОС, а также невозможность перехвата вредоносными программами контроля над защищаемой Dr.Web системой.

- **Dr.Web ShellGuard** — технология, которая закрывает путь в компьютер для эксплойтов — вредоносных объектов, пытающихся использовать уязвимости, в том числе еще не известные никому, кроме вирусописателей (т. н. уязвимости «нулевого дня»), с целью получения контроля над атакуемыми приложениями или операционной системой в целом.

63.5. История создания

История разработки антивируса Игоря Данилова начинается с 1991 года, а под маркой Dr.Web антивирусы разрабатываются и распространяются с 1994 года.

- 1992 год — создание первой версии антивирусной программы Spider's Web (прототипа Dr.Web). В ней была реализована идея выполнения кода программ в эмуляторе процессора для поиска неизвестных вирусов.

- 1993 год — участие программы Spider's Web на международной выставке CeBIT.

- 1994 год — начало продаж антивируса Doctor Web, призванный заменить популярную в то время в России антивирусную программу Aidstest, которая не могла бороться с появившимися полиморфными вирусами, полностью изменяющими свой код при каждом заражении.

- 1995 год — демонстрация Антивирусного комплекта DSAV 2.0. В комплект входит антивирус Doctor Web.

- 1996 год — дебют программы Dr.Web (версия 3.06b) на сравнительном тестировании полифагов, проводимом журналом Virus Bulletin, более чем впечатляющий — как по уровню знания полиморфных вирусов, так и по качеству эвристического анализатора. В статье журнала Virus Bulletin о программе Doctor Web (версия 3.08) был особо отмечен эвристический анализатор антивируса, который в режиме «параноик» определил 100 % полиморфных вирусов.

Представлена альфа-версия Dr.Web для Novell NetWare.

- 1997 год — впервые российская антивирусная программа (Dr.Web) вошла в тройку лучших антивирусов мира по результатам тестирования журнала Virus Bulletin. Выходит бета-версия Dr.Web для Novell NetWare.
- 1998 год — выход Dr.Web 4.0. Изменена архитектура и алгоритм работы программы. Публичное тестирование Dr.Web для Windows 95/98/NT.
- 1999 год — появление резидентного модуля SpIDer Guard для Windows 95/98. Dr.Web для Windows 95/98/NT получает первую награду VB100 в тестах журнала Virus Bulletin. Выход коммерческой версии Dr.Web для Windows 95/98/NT. В Dr.Web впервые реализована проверка памяти виртуальных машин в среде Windows NT.
- 2000 год — Dr.Web получил сертификат соответствия Минобороны РФ. Резко увеличена частота выхода обновлений вирусной базы — до нескольких раз в час.
- 2001 год — заключено соглашение с компанией Яндекс. С этого момента все письма, проходящие через почтовую систему Яндекс, проверяются с помощью решений Dr.Web.
- 2002 год — создание антивирусных фильтров Dr.Web для почтовых серверов CommuniGate Pro. Выпуск первой бета-версии Dr.Web для Unix с уникальной на тот момент функцией — лечением файлов налету. Выпуск программы SpIDer Mail — уникальной на тот момент программы для проверки входящей почты.
- 2007 год — создание технологии несигнатурного обнаружения вредоносных программ Origins.Tracing.
- 2007 год — открыто публичное тестирование сервиса Dr.Web AV-Desk, на базе которого интернет-провайдеры предоставляют своим абонентам услугу «Антивирус Dr.Web» (первая в российской сфере интернет-бизнеса SaaS-модель).
- 2008 год — появление антивирусного пакета Dr.Web Security Space. Впервые реализован новый компонент для проверки HTTP-трафика — Dr.Web SpIDer Gate.
- 2009 год — начало бета-тестирования антивирусного продукта Dr.Web Security Space Pro[12] Отличается от Dr.Web Security Space наличием сетевого экрана.
- 2010 год — выпуск первого в России антивируса под ОС Android — Dr.Web для Android.
- 2013 год — выпуск нового продукта Dr.Web Security Space 9. Новые функции Dr.Web Cloud, превентивная защита, поведенческий анализатор Dr.Web Process Heuristic, защита пользовательских данных от повреждения, комплексный анализатор упакованных угроз, проверка трафика по всем протоколам, функция «Безопасный поиск», защита общения в популярных сервисах мгновенных сообщений и другие функции.
- 2014 год — выпуск 10 версии антивируса.
- В сентябре 2015 года на Украине продукты компании попали под запрет государственных закупок товаров и услуг[13]. Некоторые СМИ ошибочно сообщили, что «санкции предусматривают блокировку активов и приостановление выполнения экономических и финансовых обязательств со стороны Украины»[14][15].
- 2015 год — в ноябре вышел Dr.Web Security Space 11, основными нововведениями которого стало усиление самозащиты и превентивной защиты, в частности, новая технология Dr.Web ShellGuard позволила обеспечить защиту от эксплойтов, использующих т. н. уязвимости «нулевого дня».
- 2015 год — выпуск продукта Dr.Web Katana (который входит в состав Dr.Web Security Space) , решения для защиты, которое сочетается с уже установленным антивирусом другого производителя.[16]

63.6. Награды

- По результатам теста на лечение активного заражения (октябрь 2008), проведённого сайтом anti-malware.ru, Dr.Web единственный из всех участников набрал максимально возможное число баллов (15) и получил Platinum Malware Treatment Award.[17]
- По результатам теста самозащиты антивирусных продуктов (январь 2009), проведённого сайтом anti-malware.ru, Dr.Web единственный из всех участников набрал максимально возможное число баллов (38) и получил Platinum Self-Protection Award.[18]
- По результатам теста проактивной защиты (март 2009), проведённого сайтом anti-malware.ru, Dr.Web занял второе место и получил награду Silver Proactive Protection Award.[19]
- Platinum Self-Protection Award (сентябрь 2010) от Anti-Malware.ru.[20]

- С определённого момента компания «Доктор Веб» отказалась от участия в сравнительных тестированиях антивирусных продуктов, аргументируя это тем, что «на их основании практически невозможно сделать объективные выводы о качестве сравниваемых продуктов, об их способности защитить пользователей от современных вирусных угроз»[21].

63.7. Инциденты, связанные с компанией «Доктор Веб»

63.7.1. Нападения на офис «Доктор Веб» и угрозы физической расправы от распространителей банкоматных троянцев

В день публикации новости о внесении в вирусные базы записи о Trojan.Skimer.18 (18 декабря 2013 г.) компания «Доктор Веб» получила угрозу предположительно от авторов троянца или от криминальной структуры, финансирующей его разработку и продвижение (орфография авторов сохранена):[22]

> ПРЕДУПРЕЖДЕНИЕ !!!
>
> От лица Синдиката поздравляем с успешным дизасемблированием программного скимера банкоматов NCR . Исходник авторов прилагаются ниже.
> Хорошая работа, но безперспективная. Прибыль от Dr.Web_ATM_shield копеечная посколько банкиры добровольно деньги никогда не отдают. Однако развитие Dr.Web_ATM_shield подрывает деятельность Синдиката с много милионной прибылью. Сотни криминальных семей по всему миру могут остаться без дохода.
>
> У вас НЕДЕЛЯ убрать все упоминания о ATM.Skimmer с вашего web ресурса. Иначе синдикат остановит операции обналички и отправит весь криминалитет за головами ваших программистов. Финал ООО DrWeb будет трагичен.

После того как требование было проигнорировано, 9 марта 2014 года имели место попытки поджога офиса «Санкт-Петербургской антивирусной лаборатории И. Данилова» (САЛД), ответственность за которые взял на себя упомянутый «синдикат».

31 марта 2014 года, после двух поджогов офиса Санкт-Петербургской Антивирусной Лаборатории Данилова, компания «Доктор Веб» получила вторую угрозу:

> Уважаемый Dr.Web, международный синдикат кардеров предупреждал вас о недопустимости вашего вмешательства в сферу АТМ. В связи с тем что вы проигнорировали требования синдиката - в отношении вас были применены санкции. Да бы подчеркнуть целеустремленность синдиката - ваш офисна ул. Благодатная был сожжен дважды.
>
> Если в течении 10 дней вы не уберете из ваших продуктов все упоминания о вирусах класса atmskimmer и все продукты для АТМ - международный синдикат кардеров уничтожит все ваши офисы по всему миру, Так же синдикат пролобирует закон о запрете использования русских антивирусов во всех странах имеющих представительства синдиката , под предлогом защиты от не-дружественых всему миру российских спецслужб.
>
> Входящие письма на данном e-mai проверяется, разумные аргументы спора будут учтены.

После третьего нападения на офис САЛД органами правопорядка был задержан подозреваемый, который был впоследствии отпущен из-за недостаточности свидетельских показаний. В то же время было предотвращено три попытки физического проникновения в московский офис компании «Доктор Веб». По словам генерального директора компании Б. А. Шарова, причина такой активности киберпреступиков заключается в том, что специалисты «Доктор Веб» обнаружили и добавили в вирусные базы запись о Trojan.Skimer.18 в очень неудачный для распространителей момент, когда разработка этого троянца для банкоматов уже завершилась, но продажи на чёрном рынке ещё не начались.[23]

В ответ на угрозы и нападения компания выпустила официальное заявление, в котором говорилось, что компания «Доктор Веб» считает своим долгом обеспечение максимальной защиты пользователей от посягательств киберпреступников, соответственно, работы, направленные на выявление и изучение угроз для банкоматов, будут продолжены, равно как и дальнейшее совершенствование продукта Dr.Web ATM Shield.[24]

63.7.2. Скандал в связи с конфискацией неофициальной фанатской группы

Летом 2015 компания оказалась в центре скандала, связанного с недружественным захватом

руководством компании неофициальной фанатской группы в социальной сети Вконтакте, и принудительным удалением создателя сообщества из администраторов.[25][26] Инициатор скандала требовал денежной компенсации или возврата сообщества.[27] По словам представителя компании, создатель группы самоустранился от участия в её развитии, и несколько лет группа развивалась и поддерживалась только штатными сотрудниками «Доктор Веб». Ещё в начале 2013 года в связи с возникающими в социальной сети «ВКонтакте» прецедентами создания пользователями групп для клиентов известных компаний, развития этих групп силами самих компаний и последующим появлением оригинальных создателей группы, сопровождающихся требованиями денежных компенсаций и угрозами удалением группы, компания обратилась к социальной сети «ВКонтакте» с просьбой передать права администрирования группы на аккаунт, принадлежащий «Доктор Веб», и просьба была удовлетворена.[28]

63.8. См. также

- Dr.Web Live CD
- ВебIQметр

63.9. Примечания

[1] Программно-аппаратные комплексы Dr.Web Office Shield.

[2] Dr.Web Enterprise Security Suite.

[3] Dr.Web® AV-Desk — wiki.drweb.com

[4] Новая версия персональных продуктов Dr.Web для Windows 7.0: высокая скорость сканирования и управление антивирусной сетью в домашних условиях. news.drweb.ru. Проверено 27 ноября 2015.

[5] Новая версия 8 Антивируса Dr.Web для Windows несет новые преимущества пользователям. news.drweb.ru. Проверено 27 ноября 2015.

[6] Новая версия Dr.Web 9.0 для Windows — версия быстрого реагирования.

[7] Новая версия Dr.Web 10.0 для Windows: полная гармония защиты. products.drweb.ru. Проверено 27 ноября 2015.

[8] Dr.Web® — инновационные технологии антивирусной безопасности. Комплексная защита от интернет-угроз.. products.drweb.com. Проверено 27 ноября 2015.

[9] Dr.Web CureIt! — Лечащая утилита. Проверено 29 марта 2013. Архивировано из первоисточника 4 апреля 2013.

[10] Отправка статистики

[11] Антивирус Dr.Web Light — второе по популярности бесплатное приложение в русском сегменте Android Market!

[12] Dr.Web® — инновационные технологии информационной безопасности. Комплексная защита от интернет-угроз

[13] Україна б'є росіян гривнею — Фінансовый клуб. finclub.net. Проверено 12 ноября 2015.

[14] УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №549/2015

[15] Под украинские санкции попали российские министры и крупнейшие авиакомпании - Новости Политики - Новости Mail.Ru

[16] Dr.Web Katana – продукт нового поколения для защиты на опережение. news.drweb.ru. Проверено 26 ноября 2015.

[17] Результаты теста антивирусов на лечение активного заражения (октябрь 2008) — Тесты и сравнения антивирусов — Anti-Malware.ru

[18] Результаты теста самозащиты антивирусов (январь 2009) — Тесты и сравнения антивирусов — Anti-Malware.ru

[19] Результаты теста проактивной антивирусной защиты (март 2009) — Тесты и сравнения антивирусов — Anti-Malware.ru

[20] Тест самозащиты антивирусов, сравнение антивирусов (сентябрь 2010) — Тесты и сравнения антивирусов — Anti-Malware.ru

[21] Заявление «Доктор Веб» относительно участия продуктов компании в сравнительном тестировании журнала Virus Bulletin. news.drweb.ru. Проверено 12 ноября 2015.

[22] Dr.Web - Троянцы для банкоматов – «Доктор Веб» и банкоматные троянцы. antifraud.drweb.ru. Проверено 13 ноября 2015.

[23] ATM Skimmer Gang Firebombed Antivirus Firm — Krebs on Security. krebsonsecurity.com. Проверено 13 ноября 2015.

[24] «На карте – ваши деньги»! Банкоматные троянцы угрожают вам, а их распространители – поджогами и физической расправой сотрудникам компании «Доктор Веб». news.drweb.ru. Проверено 13 ноября 2015.

[25] Злоупотребление правом или как легко отнять фанатское сообщество (на примере антивируса Dr. WEB)

[26] Директор по интернет-маркетингу Rambler&Co Антон Сучков порекомендовал главреду «Игромании» «отжать паблик» используя прецедент с Dr.Web

[27] Верните фанатский паблик, захваченный фирмой на незаконных основаниях, или полностью оплатите работу SMM\PR-менеджера по созданию и раскрутке сообщества и рекламе ваших продуктов!

[28] «Доктор Веб» объяснил, как он удалил из ВК-паблика его бездействующего создателя и передал права своим сотрудникам → Roem.ru. roem.ru. Проверено 13 ноября 2015.

63.10. Ссылки

- Официальный сайт
- Официальный форум
- Сервис проверки ссылок
- Сообщество пользователей Dr.Web
- Бесплатная разблокировка Windows

Глава 64

Dr.Web Live CD

Dr.Web LiveCD — оригинальный программный продукт, основанный на стандартном антивирусном сканере Dr.Web. Этот сканер позволяет восстановить систему в тех случаях, когда вследствие вирусной активности произвести загрузку компьютера с жёсткого диска обычным способом невозможно.

64.1. Основные функции Dr.Web LiveCD

До 14 августа 2014 года работал под управлением операционной системы Gentoo Linux[1], после 14.08.2014 года был создан LiveCD на основе Ubuntu с рабочим столом Mate 1.6.0, в котором через Wine 1.6 можно запустить лечащую утилиту Dr.Web *CureIt*!®. Предназначен для проверки компьютеров на базе Windows (файловые системы NTFS, FAT32 и FAT16).

Может быть запущен в одном из двух режимов: в обычном режиме с графическим интерфейсом и в безопасном режиме отладки (debug mode) с интерфейсом командной строки (консольный сканер).

Приложение способно не только очистить компьютер от различного рода вредоносных программ, но и попытаться вылечить заражённые объекты.

В приложении реализована возможность загрузки по локальной сети.

Предусмотрена возможность обновления вирусных баз через интернет-соединение. На официальном сайте ISO-образ LiveCD пересобирается с новыми вирусными базами ежесуточно.

Имеется встроенный браузер.

На некоторых конфигурациях аппаратного обеспечения Dr.Web LiveCD не загружается из-за невозможности загрузить какой-либо модуль ядра. Для решения этой проблемы сначала определите, на каком модуле происходит остановка загрузки в режиме отладки, а затем при следующей загрузке в загрузочном меню нажмите TAB и допишите в строку загрузки параметр, запрещающий грузить проблемный модуль, например raid456=no[2]

Можно также создать LiveUSB.

64.2. Примечания

[1] Dr.Web LiveCD — для Windows с помощью Linux / Dr.Web / OpenLife (недоступная ссылка с 14-05-2013 (959 дней) — *история*)

[2] Livecd проблема — Dr.Web users' forum

64.3. Ссылки

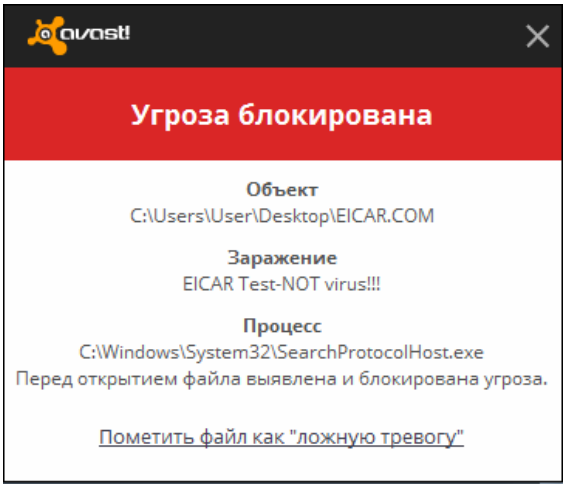
- Официальный сайт
- Dr.Web LiveUSB
- Официальный ftp

Глава 65

EICAR-Test-File

EICAR (или **EICAR-Test-File** — от **E**uropean **I**nstitute for **C**omputer **A**ntivirus **R**esearch) — стандартный файл, применяемый для проверки, работает ли антивирус. По сути вирусом не является; будучи запущенным как COM-файл DOS, всего лишь выводит текстовое сообщение и возвращает управление DOS. Программа работает в средах, поддерживающих выполнение 16-битного ПО для DOS, таких как MS-DOS, OS/2, Windows 9x и 32-битные Windows NT. Под 64-битными версиями Windows файл не запускается.

Хотя COM-файлы в общем случае являются двоичными, EICAR содержит только символы ASCII. Поэтому любой пользователь может убедиться в работоспособности своего антивируса, набрав в текстовом редакторе (например, в Блокноте) тестовую строку длиной 68 байт и сохранив её с расширением .EXE или .COM. Символы CR/LF, которые редактор может добавить в конец файла, не влияют на работу EICAR. Обычно, если резидентный монитор антивируса включен, уже после нажатия кнопки «Сохранить» выводится предупреждение.



Реакция антивируса avast! на EICAR

65.1. Реакция антивирусов

Антивирус, обнаруживший данную строку, должен поступить в точности так же, как и при обнаружении реального вируса. Поэтому о том, что тревога учебная, антивирус обычно сообщает в названии вируса:

- EICAR Test-NOT virus!!! (avast!),

  EICAR-Test-File (Антивирус Касперского),
- EICAR Test File (Not a Virus!) (Doctor Web),
- EICAR-AV-Test (Sophos),
- EICAR_Test_File (RAV),
- Eicar_test_file (Trend Micro),
- Eicar-Test-Signature (Avira AntiVir),
- EICAR_Test_File (FRISK),
- EICAR_Test (+356) (Grisoft),
- Eicar-Test-Signature (ClamAV),
- Eicar.Mod (Panda Cloud Antivirus),
- VIRUS:DOS/EICAR_Test_File (Microsoft Security Essentials).
- Eicar тест файл (NOD32)
- Teststring.Eicar (Comodo Internet Security, Comodo AntiVirus)
- EICAR_test_file (Virus) (Outpost Security Suite)

Крайне редко встречаются антивирусы, которые не реагируют на этот тест.

65.2. Для чего предназначен

Разумеется, EICAR не проверяет, насколько оперативно разработчики реагируют на вирусы и насколько качественно излечиваются заражённые файлы — для этого нужен «зоопарк» свежих вирусов. Его задача другая: продемонстрировать работоспособность антивирусной системы и указать, какие объекты проверяются антивирусом, а какие — нет. Например:

- Есть подозрение, что компьютер заражён. Действует резидентный монитор, или вирус сумел его отключить?
- Обычный почтовый червь наподобие VBS.LoveLetter должен для заражения пройти несколько стадий: загрузиться на компьютер по протоколу POP3; записаться в базу почтового клиента; по команде пользователя распаковаться во временный файл и запуститься. На какой стадии он будет замечен?
- Существует много способов «протащить» вредоносную программу мимо «глаз» антивируса: закодировать в Base64, вложить в OLE-объект Microsoft Word, в RAR, JPEG, сжать упаковщиком наподобие UPX. Что из этого антивирус распакует?
- Кроме того, антивирусы бывают не только локальные, но и сетевые — проверяющие сетевой трафик; при ошибке конфигурирования они будут либо загружать сервер излишней работой, либо, наоборот, пропускать вредоносные файлы.

Для того, чтобы проверить, какова будет реакция антивируса, конечно, можно применить и «живой» вирус — но это «как поджигание урны для проверки пожарной сигнализации».[1] Для этого и был предложен стандартизированный файл, не несущий вредоносной нагрузки.

65.3. COM-файл

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Этот COM-файл при запуске выводит сообщение:

EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

после чего возвращает управление DOS.

65.4. Примечания

[1] Сайт EICAR

65.5. См. также

- GTUBE
- Официальный сайт

Глава 66

Emsisoft Anti-Malware

Антивирус и анти-spyware защита, разработанные в Австрии на основе программного обеспечения Emsi (Gesellschaft mit beschränkter Haftung GmbH). Переименована в Emsisoft Anti-Malware.

Является проприетарным. Данный антивирус защищает от классических вирусов, троянов, ботов (включая рекламных), шпионского и рекламного ПО, а также keylogger'ов. A-squared Anti-Malware содержит резидентных сторожей. По утверждениям разработчиков их продукт не только не замедляет систему, а наоборот ускоряет её.

66.1. Особенности

ВЕБ-ЗАЩИТА: Когда вы пытаетесь получить доступ к опасным сайтам с вредоносным ПО, Emsisoft Anti-Malware будет блокировать такие действия. Встроенный список опасных сайтов автоматически обновляется каждый час.

ФАЙЛОВАЯ ЗАЩИТА: Этот важнейший компонент проверяет все загружаемые и запускаемые программы. Файловая защита Emsisoft Anti-Malware очень умна и оптимизирована, поэтому, вы не почувствуете высокой нагрузки программы во время фоновой работы.

АНАЛИЗАТОР ПОВЕДЕНИЯ: Чтобы защитить вас еще от неизвестных угроз, Emsisoft Anti-Malware следит за всеми программами, и в случае опасных действий, сообщает об этом в уведомлении. Работая вместе с облачной сетью сообщества Emsisoft Anti-Malware, продукт является мощной защитой против вирусных атак.

66.2. Ссылки

- Описание Anti-Malware (русский язык)
- ПиСиМэгезин — статья об A-square
- - A-square

Глава 67

EScan Antivirus

eScan Antivirus — программное решение для защиты от вирусов и обеспечения безопасности контента в режиме реального времени. **eScan** фактически блокирует угрозы до их попадания на компьютер — то есть до того, как они могут сохраниться на жесткий диск или передаться приложениям. Антивирусы семействае Scan разрабатываются компанией eScan MicroWorld. **eScan** обеспечивает защиту рабочих станций и серверов от вирусов (в том числе угроз «нулевого дня»), нежелательного и неподобающего интернет-контента, а также от других угроз безопасности, таких как шпионское ПО, рекламное ПО, клавиатурные шпионы, руткиты, бот-сети, хакерские атаки, спам и фишинг.

67.1. Уникальные технологии eScan

Благодаря использованию технологии **MWL** (MicroWorld Winsock Layer) продукты eScan нейтрализуют все угрозы ещё на сетевом уровне, до того, как они могут достичь приложений на компьютере. **MWL** проверяет входящие пакеты данных, передаваемые по сети, детектируя вредоносные программы на уровне сокетов операционной системы Microsoft Windows (Winsock). Таким образом достигается высочайший уровень защиты Вашего компьютера.

Сложные эвристические алгоритмы обнаружения вредоносных программ позволяют нейтрализовать не только известные, но также новые, только что появившиеся угрозы, для которых ещё не существует сигнатур. Все обнаруженные угрозы полностью излечиваются.

Технология **Non-Intrusive Learning Pattern** (NILP), использующая методы искусственного интеллекта, позволяет продуктам eScan эффективно отсеивать спамерские и фишинговые электронные письма. **NILP** содержит механизм адаптации к поведению пользователя и анализа того, какие сообщения для пользователя являются желательными, а какие нежелательными.

Технология **Domain and IP Reputation Checker** (DIRC) проверяет репутацию любых подозрительных веб-сайтов и IP-адресов, надежно защищая от фишинга, вредоносных программ, нежелательного контента, хакерских атак и других актуальных угроз.

67.2. Функциональность eScan

Базовая защита:

- защита от известных вредоносных программ;
- эвристическая проактивная защита от новых угроз;
- защита от спама;
- межсетевой экран;
- защита от руткитов, шпионского и рекламного ПО;
- фильтр фишинга;
- игровой режим;
- защита папок и пользовательская блокировка файлов;
- мониторинг сетевой активности;
- автоматическая загрузка критических патчей Windows;
- автоматические обновления.

Всесторонняя защита — для активных пользователей eScan предлагает дополнительные функции:

- проверка веб-трафика;
- блокирование опасного веб-контента, апплетов и скриптов;
- защита съёмных устройств и контроль приложений;
- виртуальная клавиатура.

67.3. Высокое быстродействие

MWL — очень быстрая и малоресурсоёмкая технология. В продуктах eScan, детектирующих угрозы на сетевом уровне, сведены к минимуму достаточно ресурсоемкие операции обращения к файловой системе. Благодаря этому продукты eScan отличаются хорошей производительностью и практически не замедляют работу компьютера. В режиме ожидания eScan потребляет всего около 20 МБ оперативной памяти!

67.4. Системные требования

Процессор: Pentium II 200 МГц

- RAM: 256 МБ (512 МБ рекомендуется);
- Hard Disk: не менее 300 МБ свободного пространства;
- Internet Explorer 6.0 и выше;
- CD-ROM.

Операционная система

- Windows 8 / 7 / Vista / XP;
- Windows 2008 / 2003 / 2000 (Workstation & Server);
- Все версии 32 & 64 бит.

67.5. Награды

По состоянию на август 2012 года eScan имеет более 30-и наград VB100% авторитетного издания Virus Bulletin.

2012 год:

- eScan Anti-Virus 11.0 получил высшую награду ADVANCED+ по итогам тестирования AV-Comparatives, март 2012;
- eScan Internet Security получил ряд престижных наград «VB100» по итогам тестов, проведенных лабораторией VirusBulletin как на платформе Windows, так и Linux;

2011 год:

- Антивирус eScan получил высокий уровень сертификации Advanced по результатам тестирования AV-Comparatives;
- Антивирус eScan Internet Security Suite 11 признан русскоязычной версией журнала PC Magazine одной из лучших программ 2011 года;
- Независимая тестовая лаборатория VirusBulletin на протяжении года неоднократно подтверждала высокое качество и эффективность работы eScan;
- Антивирус eScan ISS по итогам тестирования AV-Comparatives в августе 2011 года стал лидером среди лучших продуктов для защиты доступа к конфиденциальным данным пользователей;
- eScan Anti-Virus 11: отличные результаты в тесте AV-Comparatives February 2011
- eScan получил высокую оценку в тестировании VB100 RAP testing (Reactive And Proactive)

67.6. Утилита eScan AntiVirus Toolkit (MWAV)

eScan предлагает бесплатную утилиту, сканирующую и удаляющую вирусы, троянские, шпионские, рекламные и другие вредоносные программы, которыми мог быть инфицирован компьютер. Утилита eScan Antivirus Toolkit не требует установки и может быть запущена непосредственно с компьютера, USB-носителя или с CD. Она может быть запущена, даже если на вашем компьютере уже установлена другая антивирусная программа.

eScan Antivirus Toolkit регулярно обновляется до последней версии для оперативного обнаружения и удаления недавно выпущенных троянских, шпионских, рекламных и других вредоносных программ.

Антивирусный сканер MWAV:

- детектирует все типы вредоносных программ — вирусы, руткиты, троянцев, компьютерных червей, рекламное и шпионское ПО;
- лечит компьютер от обнаруженных угроз;
- может запускаться из командной строки и выбором параметров сканирования;
- может быть добавлен в список автозагрузки;
- получает последние обновления при каждом запуске;
- проверяет архивы;
- использует эвристику и другие методы обнаружения нового вредоносного ПО, для которого ещё нет специализированных сигнатур.

MWAV поддерживает все актуальные версии операционных систем Windows и не конфликтует с другим программным обеспечением, в том числе антивирусным. eScan AntiVirus Toolkit (MWAV) имеется на установочном диске с продуктом eScan.

67.7. Ссылки

- Официальный сайт eScan
- Руководство пользователя eScan Internet Security Suite
- Полезная информация по продуктам eScan
- Видеокурс по установке, настройке и управлению продуктами eScan

Глава 68

ESET NOD32

ESET NOD32 — антивирусный пакет, выпускаемый словацкой фирмой ESET. Первая версия была выпущена в конце 1987 года[3]. Название изначально расшифровывалось как «Nemocnica na Okraji Disku» («Больница на краю диска», перефраз названия популярного тогда в Чехословакии телесериала «Больница на окраине города»).

ESET NOD32 — это комплексное антивирусное решение для защиты в реальном времени. ESET NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы[4], черви, spyware, adware, фишинг-атаки. В ESET NOD32 используется патентованная технология ThreatSense, предназначенная для выявления новых возникающих угроз в реальном времени путём анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ.

При обновлении баз используется ряд серверов-зеркал, при этом также возможно создание внутрисетевого зеркала обновлений, что приводит к снижению нагрузки на интернет-канал. Для получения обновлений с официальных серверов необходимы имя пользователя и пароль, которые можно получить, активировав свой номер продукта на странице регистрации регионального сайта.

Наравне с базами вирусов NOD32 использует эвристические методы, что может приводить к лучшему обнаружению ещё неизвестных вирусов.

Большая часть кода антивируса написана на языке ассемблера[5], поэтому для него характерно малое использование системных ресурсов[6][7] и высокая скорость проверки с настройками по умолчанию[8][9].

68.1. Состав версий 2. x и 3. x

Antivirus MONitor (AMON)

Резидентный сканер, который автоматически проверяет файлы при доступе к ним.

NOD32

Сканер по запросу, который можно запустить вручную для проверки отдельных файлов или разделов диска. Этот модуль также может быть запущен в часы с наименьшей загрузкой с помощью планировщика.

Internet MONitor (IMON)

Резидентный сканер, работающий на уровне Winsock и препятствующий попаданию зараженных файлов на диски компьютера. Данный модуль проверяет HTTP-трафик и входящую почту, получаемую по протоколу POP3. Данный модуль в версиях 2.x может конфликтовать с некоторыми службами Windows Server и с некоторыми межсетевыми экранами (например, Kerio WinRoute). При установке система исследуется на возможность конфликтов и, если существует вероятность конфликта, выводится сообщение, предлагающее отключить этот компонент.

E-mail MONitor (EMON)

Дополнительный модуль для проверки входящих/исходящих сообщений через интерфейс MAPI, например, в Microsoft Outlook и Microsoft Exchange.

Document MONitor (DMON)

Использует запатентованный интерфейс Microsoft API для проверки документов Microsoft Office (включая Internet Explorer).

68.2. Состав версии 4.x

Модуль защиты от вирусов и шпионских программ

В этом модуле используется ядро сканирования на основе технологии ThreatSense. Ядро ThreatSense оптимизировано и улучшено в соответствии с требованиями новой архитектуры ESET Smart Security.

Персональный брандмауэр

Персональный брандмауэр отслеживает весь трафик между защищаемым компьютером и другими компьютерами сети.

Модуль защиты от нежелательной почты

Модуль защиты от нежелательной почты ESET фильтрует нежелательную почту, повышая уровень безопасности системы и удобство использования обмена данными по электронной почте.

ESET SysRescue

ESET SysRescue позволяет пользователям создавать загрузочный носитель CD, DVD или USB с программой ESET Smart Security, который может запускаться независимо от операционной системы. Он предназначен главным образом для работы с трудноудаляемыми вирусами.

ESET SysInspector

Когда для отправки запроса в службу поддержки клиентов используется раздел «Справка и поддержка», можно добавить снимок состояния компьютера в ESET SysInspector.

Защита документов

Функция защиты документов сканирует документы Microsoft Office перед их открытием, а также проверяет файлы, автоматически загружаемые браузером Internet Explorer, например элементы Microsoft ActiveX.

68.3. Состав версии 5.x

Все функции предыдущей версии, а также

ESET Live Grid

Обеспечивают надежную защиту от Интернет-угроз и вредоносных программ в режиме реального времени.

Parental Control

Защищает Вашу семью от потенциально нежелательного веб-контента, блокируя определенные категории веб-сайтов.

Enhanced Media Control

Автоматическое сканирование всех USB-носителей, карт памяти, CD/DVD-дисков. Блокировка медиа носителей в зависимости от типа носителя, производителя, размера и других параметров.

Advanced HIPS Functionality

68.4. Позволяет настраивать поведение системы в целом и каждой её части. Пользователи могут установить правила для системной регистрации, процессов, приложений и файлов.

Gamer Mode

Обеспечивает автоматический переход в «беззвучный» режим во время работы в полноэкранном режиме.

Optimized Startup Procedure

Новое поколение продуктов ESET минимально влияет на процесс загрузки компьютера, что позволяет пользователю незамедлительно начать работу.

68.5. Состав версии 6.x

Все функции предыдущей версии, а также

Idle-State Scanning

Технология дает возможность автоматически включать сканирование в то время, когда компьютер пребывает в состоянии блокировки, либо завершения работы. В результате достигается повышенная производительность системы в целом.

Anti-Theft

Функция Антивор позволяет обнаружить местоположение и вернуть потерянный или украденный ноутбук или компьютер.

ESET Social Media Scanner

Модуль защиты для социальных сетей Facebook и Twitter.

68.6. Состав версии 7.x

Все функции предыдущей версии, а также

Enhanced Operation Memory Scanning

Технология защищает пользователя от скрытой установки шпионского и вредоносного программного обеспечения на компьютер.

Exploit Blocker

Технология «Защита от эксплойтов» - это эффективный метод обнаружения неизвестных угроз и уязвимостей нулевого дня в популярных программных продуктах. Она фокусируется на наиболее распространённом ПО, включая веб-браузеры, PDF-редакторы, почтовые клиенты, документы Microsoft Office.

68.7. Состав версии 8.x

Все функции предыдущей версии, а также

Botnet Protection

Новый модуль «Защита от ботнетов» в комплексном решении ESET NOD32 Smart Security распознает кибератаки, защищает от проникновения вредоносных ботнет-программ, предотвращает сетевые атаки и спамерские рассылки.

Enhanced Exploit Blocker

Технология «Защита от эксплойтов» уже зарекомендовала себя как эффективный метод обнаружения неизвестных угроз и уязвимостей нулевого дня в популярных программных продуктах. Она фокусируется на наиболее распространённом ПО, включая веб-браузеры, PDF-редакторы, почтовые клиенты, документы Microsoft Office. Новое поколение ESET NOD32 защищает также от атак на ПО на основе Java.

68.8. Состав версии 9.x

Все функции предыдущей версии, а также

Защита интернет-банкинга

Данная функция автоматически определяет, когда пользователи посещают сайты интернет-банкинга или страницы оплаты платежных систем и запускает защищенный браузер, чтобы обеспечить проведение транзакций в безопасной и защищенной изолированной среде.

Поддержка сетевых подписей

Сетевые подписи позволяют быстро обнаружить и заблокировать вредоносный трафик, связанный с ботами и эксплойтами. Данную функцию можно рассматривать как **Botnet Protection v2.0**.

Обновленный пользовательский интерфейс

Пользовательский интерфейс получил значительно измененный дизайн и был упрощен на основе результатов тестирования юзабилити. Все текстовые сообщения и уведомления были тщательно пересмотрены. Интерфейс содержит поддержку иврита и некоторых арабских языков (чтение справа налево), а также динамически обновляемый онлайн файл справки.

68.9. Защита от фишинга

- Присутствует во всех версиях антивируса для Windows

Данная функция защищает пользователя от фишинг-страниц и онлайн угроз

68.10. Хронология версий

- 1992 (?) год — NOD для MS-DOS.
- **1998 год — NOD32 1.0 для Windows 95.**
- 1999 (?) год — NOD32 1.5 для Windows 98.
- **2003 год — NOD32 2.0 для Windows XP.**
- **Ноябрь 2007 — NOD32 3.0 для Windows XP, Vista.** Разделение на “NOD32 Antivirus” и “NOD32 Smart Security”.
- **Март 2009 — NOD32 4.0 для Windows XP, Vista.** Добавлены модули “ESET SysInspector” и “ESET SysRescue”.
- **Август 2010 — NOD32 4.2 для Windows XP, Vista, 7.**
- Май 2011 — начало beta-тестирования NOD32 версии 5.0 для Windows 2000, XP, Vista, 7, Home Server.
- **Сентябрь 2011 — официальный релиз NOD32 версии 5.0 (5.0.93.15).**
- Весна 2012 — начало beta-тестирования NOD32 версии 6.0 для Windows XP, Vista, 7, Home Server.
- **Декабрь 2012 — официальный релиз NOD32 версии 6.0 (6.0.304.6).** Добавлен модуль "Антивор".
- Март 2013 — релиз обновлённой 6.0.314.2 версии NOD32 с небольшими исправлениями.
- Апрель 2013 — релиз обновлённой 6.0.316.0 версии NOD32 с небольшими исправлениями.

- Июнь 2013 — начало beta-тестирования NOD32 версии 7.0 для Windows XP, Vista, 7, 8, 8.1, Home Server.
- **Ноябрь 2013 — официальный релиз NOD32 версии 7.0 (7.0.302.8).** Добавлена проверка оперативной памяти и блокировка злоупотреблений известными эксплойтами.
- Август 2014 — начало beta-тестирования NOD32 версии 8.0 для Windows XP, Vista, 7, 8, 8.1, Home Server.
- **Ноябрь 2014 — официальный релиз NOD32 версии 8.0 (8.0.304.1).** Добавлена блокировка эксплойтов на основе Java и защита от ботнетов (ESS).
- Май 2015 — начало beta-тестирования NOD32 версии 9.0 для Windows XP, Vista, 7, 8, 8.1, 10, Home Server.
- Июль 2015 — релиз обновлённой 8.0.319.1 версии NOD32 с небольшими исправлениями.
- **Октябрь 2015 — официальный релиз NOD32 версии 9.0 (9.0.318.20).** Добавлена защита интернет-банкинга, поддержка сетевых подписей и обновлен пользовательский интерфейс.

68.11. Поддерживаемые платформы

- Windows 10, 8.1, 8, 7, Vista, XP (до 2017 года[10]), ME, 98 и 95[*источник не указан 450 дней*]; Windows Home Server 2003, Windows Home Server 2011
- OS X[11]
- MS-DOS[*источник не указан 450 дней*]
- Linux
- Android[12] (Заявлена поддержка устройств с Android 2.2)

68.12. Интересные факты

- Из участников тестирования Virus Bulletin 100 % Eset NOD32 обладает наибольшим среди тестируемых (80 по состоянию на Июль 2013 года) количеством наград данной лаборатории.
- Компактный размер обновлений (размер измеряется десятками килобайт).
- Поддержка баз и модулей до сих пор осуществима для 3.x,4.x-версии, прекращение обслуживания которых до сих пор не оговорено, так как у них идентичное ядро с новейшими версиями.
- Единственный антивирусный продукт, который не изменил дизайн за 5 лет.
- В ESET при включенном “LIveGrid” можно смотреть отчёт, отслеживая информацию, переданную в компанию.
- Полная интеграция и подмена собой фаервола (брандмауэра).
- Согласно проведенным тестам отдельных пользователей в просторах СНГ, функции социальных сетей и "Антивор" признаны ненужными и более того - неэффективными. Следите за своим ноутбуком и телефоном сами.
- Разработчиком заявлена поддержка Windows 10

68.13. Примечания

[1] Does Your Anti-Threat Software Actually Protect - Bogus Testing Methods. Complete Transcript of Randy Abram – ESET Interview

[2] (NOD32) an extremely fast Hi-Performance Scanning Engine. Complete Transcript of Randy Abrams – ESET Interview

[3] О компании ESET

[4] Описания, антивируса

[5] ESET — Essential Security against Evolving Threats

[6] Wilders Security Forums — View Single Post — Fun with NOD32

[7] Wilders Security Forums — View Single Post — memory utilisation

[8] ESET's NOD32 Achieves 34th Consecutive Virus Bulletin 100 % Award; NOD32 Is Recognized for Flawless Virus Protection; Performs Scans Five Times Faster than Symantec Antivirus Business Wire

[9] ESET NOD32 Wins Virus Bulletin 100 % Award Once Again Newswire

[10] ESET не бросает пользователей Windows XP (рус.). Пресс-центр ESET (4 апреля 2014). Проверено 8 октября 2014.

[11] ESET выпускает антивирусное решение NOD32 для Mac (рус.), *Пресс-центр ESET* (24 ноября 2010). Проверено 8 октября 2014.

[12] ESET NOD32 Mobile Security защищает смартфоны под управлением Android (рус.), *Пресс-центр ESET* (31 октября 2011). Проверено 8 октября 2014.

68.14. Ссылки

- Официальный сайт
- Официальный русский сайт

Глава 69

F-PROT Antivirus

F-PROT Antivirus — антивирусная программа от исландской компании FRISK. Первая версия 3.11b была выпущена 20 декабря 2001 г[1].

69.1. Функционал

F-PROT Antivirus обеспечивает защиту компьютера с помощью сигнатурного обнаружения, а также эвристических методов[2]. Продукт обеспечивает защиту от установки модулей ActiveX, осуществляет проверку почты[2].

69.2. Распространение

Антивирус распространяется по цене $29 за лицензию на 5 компьютеров (около $6 за компьютер)[3].

69.3. Примечания

[1] Release dates of all versions of F-PROT Antivirus versions — F-PROT Antivirus

[2] http://www.f-prot.com/download/datasheets/DS-WIN-0610-01.pdf

[3] F-PROT Antivirus

69.4. Ссылки

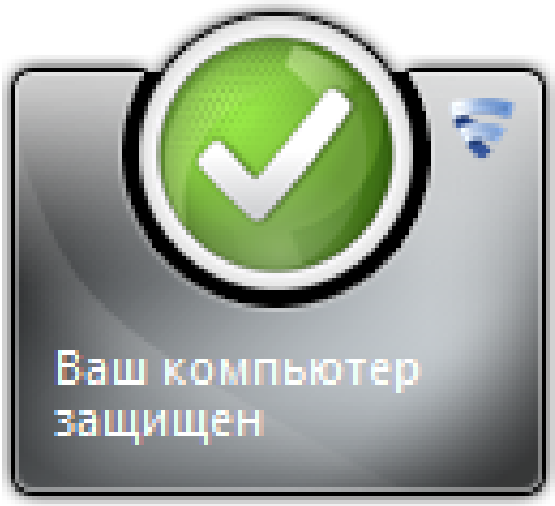
- Официальный сайт

Глава 70

F-Secure Anti-Virus

Данный антивирус антивирусная программа от финской компании F-Secure. Антивирус сочетает в себе как сигнатурное обнаружение с помощью ядра BitDefender, так и собственные разработки компании, нацеленные на обнаружение неизвестных вирусов[1][2]. До версии 2010 использовалось ядро от Лаборатории Касперского[1].

70.1. Функционал



Гаджет

- Защита от вирусов, червей и другого вредоносного ПО[3].
- DeepGuard — защита от неизвестных вирусов.

Также F-Secure Anti-Virus выводит на экран гаджет, сообщающий о текущем состоянии защиты.

70.2. Распространение

Стоимость F-Secure Anti-Virus составляет €65,90 за один год на 3 компьютера (около €22 за компьютер)[3]. Имеется версия на русском языке. На территории России распространяется как "СТРИМ.Антивирус" [4] и выступает как брендированный продукт провайдера "СТРИМ" от ОАО "КОМСТАР-Регионы" (Группа компаний ОАО "МТС"). Средняя цена за месяц подписки по России составляет 105 рублей. В 2011г. после поглощения компанией ОАО "МТС" компании ОАО "КОМСТАР-Регионы", на территории России продукт стал распространяться под брендом ОАО "МТС" и получил название "МТС Антивирус".С 2013 года появилась русская версия продуктов F-Secure, которые можно приобрести на официальном сайте производителя. Средняя цена на год комплексного решения F-Secure Internet Security на один компьютер составляет 1000 рублей. При продлении предоставляется скидка свыше 30 процентов.

70.3. Примечания

[1] F-Secure Internet Security 2010 Review: Free Download

[2] Summary Report 2009 - AV-Comparatives

[3] Buy F-Secure Antivirus to protect your online life

[4] CNews: ОАО «Комстар-Регионы» обновил «Стрим.Антивирус»

70.4. Ссылки

- Официальный сайт
- Официальный сайт "МТС Антивирус" - адаптированная версия F-Secure для России

Глава 71

G-DATA

G Data Software AG — немецкая компания, производитель программного обеспечения, специализирующаяся на IT-безопасности. Основана в 1985 году, главный офис расположен в городе Бохум (Германия). В 2009 году в компании трудилось около 250 сотрудников.

71.1. История предприятия

- 1985 год: Основание предприятия Каем Фигге и Франком Кюном. До 1987 года компания занималась разработкой программного обеспечения для Atari ST. Было разработано первое антивирусное программное обеспечение для Atari ST. Возможно, G Data является первым производителем антивирусного программного обеспечения в мире.
- 1990 год: Разработка программного обеспечения для IBM PC-совместимых ПК; оптимизация AntiVirenKit под MS-DOS.
- 1993 год: GeoRoute, первый планировщик маршрута с «интеллектуальной» картой
- 1997 год: Logox, устройство речевого вывода для Windows[1]
- 2000 год: Преобразование предприятия в акционерное общество.
- 2002 год: Создание G DATA Security и внедрение технологии «двойного сканирования».
- 2003 год: Выход на рынок Японии
- 2004 год: Представление продукта «InternetSecurity» на выставке CeBIT
- 2005 год: Внедрение технологии OutbreakShield (независимая защита от эпидемий спама и незнакомых вирусов, приходящих по электронной почте)
- 2006 год: Утверждение компании в интернациональном масштабе: появление на рынках различных стран.
- 2007 год: Программа InternetSecurity во второй раз становится победителем Штифтунг Варентест (немецкая независимая испытательная организация, созданная для обеспечения потребителей независимой, объективной информацией о товарах на основании сравнительных испытаний продукции и инспектирования услуг, проводимых в соответствии с научно обоснованными методиками, что должно было помочь потребителям избежать лишних затрат благодаря достоверной информации о качестве и цене); Открытие японского филиала в Токио.
- 2008 год: Появление на рынках Бразилии и Мексики
- 2009 год: Программа побеждает в тестировании Virus Bulletin[2]; Выход G Data на рынок России.

71.2. Самые известные продукты компании

71.2.1. Персональные решения

- G DATA AntiVirus 2014 (ранее AntiVirenKit)
- G DATA InternetSecurity 2014
- G DATA TotalCare (с 2007)
- G DATA NotebookSecurity (с 2008)
- G DATA InternetSecurity для нетбуков
- G DATA DaViDeo, программа для записи и копирования (не развивается далее)
- G DATA Total Protection 2014 (с 2013)

71.2.2. Бизнес решения

— G DATA AntiVirus Business 2010

— G DATA ClientSecurity Enterprise 2010

— G DATA ClientSecurity Business 2010

— G DATA AntiVirus Enterprise 2010

— G DATA MailSecurity 2010

Программное обеспечение продаётся в 46-ти странах мира. Среди них — Германия, Австрия, Швейцария, Италия, Франция, Бельгия, Испания, Великобритания, Нидерланды, США, Япония и Россия.

71.3. Особенности продуктов G Data

Технологии:

— *OutbreakShield (Защита от эпидемий)*

OutbreakShield реагирует на появление вирусов моментально и блокирует инфицированные письма в реальном времени — независимо от обновлений антивирусных сигнатур. Продукты компании G Data обеспечивают моментальную защиту через 0, 5 — 2 минуты с момента возникновения эпидемии. Программное обеспечение G Data реагирует на появление вирусов и действует намного быстрее чем любое другое антивирусное программное обеспечение.

— *Технология двойного сканирования*

Один антивирусный сканер не сможет обеспечить надёжную защиту. Два антивирусных движка дополняют друг друга. АнтиВирус G Data осуществляет одновременную проверку с помощью двух, одних из лучших в мире антивирусных движков. Уникальная технология двойного сканирования позволяет производить основательное распознавание вирусов и предлагает наилучшую защиту.

— *Вайтлистинг*

Известные файлы от проверенных производителей (например, системные файлы Microsoft) не проверяются программным обеспечением G Data на наличие вирусов. Таким образом ускоряется процесс сканирования, а в важных данных не обнаруживаются ошибки.

— *Фингерпринтинг*

Фингерпринтинг — это самообучающаяся технология, благодаря которой не производится повторное сканирование данных. Результаты сканирования файлов при каждом последующем сканировании сравниваются с, так называемыми, «отпечатками». «Чистый» файл проверяется после обновления сигнатур. Временной промежуток до повторной проверки каждый раз увеличивается. Так программное обеспечение G Data «учится», и, следовательно, проверка компьютера с каждым разом производится быстрее.

Возможности:

— Сетевой файрвол с возможностью централизованного администрирования.

— Встроенный *модуль G DATA backup* (G DATA TotalCare Security, G DATA Notebook Security) с возможностью использования дискового пространства на FTP-серверах G DATA из расчета 1 GB на каждую лицензию с целью резервного копирования данных.

— Встроенный *модуль file shredder (файловый шредер)*, обеспечивающий безвозвратное удаление данных без возможности восстановить их с помощью утилит восстановления данных. Модуль доступен в следующих продуктах: G DATA TotalCare Security, G DATA Notebook Security, G DATA Internet Security.

— Возможность создания *антивирусного загрузочного диска*, предназначенного для проверки жесткого диска без загрузки операционной системы.

— Специальный модуль в продукте для защиты ноутбуков (G DATA Notebook Security), предназначенный для создания *виртуального сейфа для шифрования и расшифровки данных* в режиме реального времени.

— *Модуль Tuner* с возможностью оптимизации операционной системы. Уведомления о необходимости обновления операционной системы, регулярная дефрагментация жесткого диска, периодическое удаление лишних строк реестра Windows и временных файлов, а также многие другие полезные функции.

71.4. Награды

PC Advisor Best Buy 09/09

Производит самое точное распознавание и удаление вредоносных программ, а также показывает лучшие результаты в тестированиях других категорий. Также в продукт G Data включено больше функций защиты, чем в продукты других производителей.

Протестирована версия: G Data InternetSecurity 2010

PC World Testsieg 07

ПО G Data стало лучшим при обнаружении и удалении вредоносных программ. G Data показывает лучшие результаты в тестированиях и предлагает больше функций защиты, чем многие другие продукты. Хорошее качество по доступной цене.

Протестирована версия: G Data InternetSecurity 2010

PC-Magazin Top-Produkt — 5/2009

Компания G Data предложила очень хорошую программу.

Протестирована версия: G Data InternetSecurity 2010

AwardCorporate

Протестированы версии:

G Data AntiVirus BusinessEnterprise 2010; G Data

ClientSecurity BusinessEnterprise 2010; G Data MailSecurity 2010.

AV Comparatives 2009

"Продукт G Data AntiVirus 2010 лучше всех распознаёт компьютерных вредителей. Решение безопасности G Data обеспечивает уровень распознавания 99,8 %, чем создаёт конкуренцию всем продуктам, занимающим нижние позиции в рейтинге.

Протестирована версия: G Data AntiVirus 2010

Computer Hoy PRECIO-CALIDAD

Продукт G Data Total Care 2010 обеспечивает высокий уровень распознавания вредоносных программ, легко управляем и функционирует с невероятно быстрой скоростью.

Протестирована версия: G Data Total Care 2010

Computer Hoy CALIDAD

Продукт G Data Total Care 2010 обеспечивает высокий уровень распознавания вредоносных программ, легко управляем и функционирует с невероятно быстрой скоростью.

Протестирована версия: G Data TotalCare 2010

71.5. Примечания

[1] c't 15/1997, S. 62

[2] Комплексный тест Virus Bulletin

71.6. Ссылки

- Официальная страница (англ.)
- Официальная страница (рус.)
- Дистрибьютор в России (рус.)
- Продажи решений G Data для персональных и корпоративных пользователей (рус.)
- Страница с сайта safetygate.ru (рус.)

Глава 72

Graugon Antivirus

Graugon **AntiVirus** это антивирус на основе ClamAV, разработан и поддерживается компанией Graugon Software Group. Программное обеспечение претерпело изменение имени в середине 2008 года.

72.1. История

Graugon AntiVirus был впервые выпущен в 2003 году как AntiVirus тогдашним HD1988 Labs. Программное обеспечение изначально предназначено для сканирования сетей на всё, что во вред компьютеру, в основном на вирусы. В 2005 году, HD1988 Labs объединились с другой командой-разработчиком ПО, и AntiVirus был переименован в Graugon AntiVirus.

72.2. Отзывы

По состоянию на май 2010 года Graugon AntiVirus имеет средний рейтинг пользователь 2,3 из 5 звезд по данным Fileforum.

72.3. См. также

- ClamAV

72.4. Ссылки

- Graugon AntiVirus Официальный сайт
- паб CNET профиля в Graugon
- Graugon AntiVirus обзор

Глава 73

ICSA Labs

Логотип ICSA Labs

ICSA Labs (ранее известное как Международная ассоциация Computer Security) — независимое подразделение Cybertrust Inc, занимается исследованиями, испытаниями и сертифицированием продуктов безопасности (в настоящее время более 95 % антивирусов и файрволлов и т. п. имеют сертификат ICSA) включая антивирусы, файрволлы, средства криптографии, антишпионские программы и т. д.

73.1. Ссылки

- Антивирусная программа
- Межсетевой экран

73.2. Ссылки

Официальный сайт организации

Глава 74

IKARUS Security Software

IKARUS Security Software — бренд антивирусного программного обеспечения, разработкой которого с 1986 года занимается одноименная австрийская компания IKARUS Security Software Ges.m.b.H.

74.1. История

IKARUS Security Software Ges.m.b.H была основана в 1986 году, когда проблема компьютерных вирусов имела преимущественно научно-теоретический характер. В связи с этим, компанией был создан язык для описания вирусов ViDL (Virus Description Language), который сегодня стал одним из стандартов International Computer Security Association (ICSA).

IKARUS Security Software является одной из немногих компаний, начавших разрабатывать антивирусные программы ещё до того, как в 1987 году начались первые масштабные эпидемии заражения компьютеров, привлекшие внимание СМИ к теме компьютерных вирусов.

Офис компании находится в Вене. Продукция компании хорошо известна в Европейском союзе, в частности, в Австрии, где антивирусными решениями IKARUS пользуется большинство крупнейших компаний.[1] Президентом IKARUS Security Software Ges.m.b.H является г-н Joe Pichlmayr.

Основные программные решения ИКАРУС имеют интерфейс на русском, английском, немецком и других языках.

74.2. Основные программные продукты

IKARUS virus.utilities — антивирусная программа, которая обезвреживает вирусы, сетевые черви, троянские программы и т. д., благодаря оригинальной технологии сканирования IKARUS T3.

Девиз антивируса — «virus.utilities — параноидальный антивирус не для домохозяек».[2]

IKARUS security.manager — полнофункциональное решение для офисных компьютерных сетей. Позволяет администратору управлять, конфигурировать, обновлять и контролировать продукты ИКАРУС на клиентских рабочих станциях.

IKARUS my.mailwall — проверяет электронные письма на спам и вирусы в скан-центре ИКАРУС и доставляет очищенными от вирусов и другого вредоносного кода виде.

IKARUS security.proxy — прокси-сервер. Антивирусная защита почтовых и интернет-шлюзов, работает с любым межсетевым экраном (файрволом) и не требует изменений в установках персональных компьютеров пользователей.

74.3. Примечания

[1] Telekom Austria Group: mobilkom austria Launches a Network-Based Security Solution as the First Mobile Operator Worldwide

[2] Ikarus virus utilities — антивирус ИКАРУС

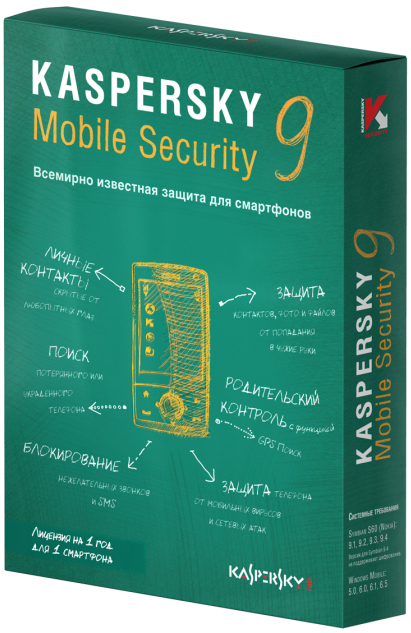
74.4. Ссылки

- Официальный сайт
- Русскоязычный сайт
- Сравнение антивируса IKARUS с другими по данным независимой тестирующей лаборатории PC Security Labs

Глава 75

Kaspersky Mobile Security

Kaspersky Mobile Security — программа для защиты смартфонов и КПК от сетевых атак, вредоносного ПО для мобильных платформ и SMS-спама, а также для защиты данных, находящихся на смартфоне, в случае его потери. Работает на платформах Symbian, Windows Mobile и Android.



Упаковка Kaspersky Mobile Security 9

75.1. Преимущества

- Блокировка телефона, в случае потери или кражи, а также возможность удалённо определить местонахождение устройства с помощью GPS.
- Шифрование данных.
- Защита от мобильных вирусов в режиме реального времени.
- Автоматическое обновление антивирусных баз.
- Ограничение исходящих вызовов и SMS-сообщений — функция «Родительский контроль».
- **Анти-вор.** Если ваш телефон потерян или украден, вы сможете его удаленно Заблокировать, сделав свои данные недоступными для посторонних. Для этого достаточно отправить SMS с паролем на свой номер. При необходимости вы также сможете Удалить данные на смартфоне, отправив на него специальное SMS. Также при удаленной блокировке на экране смартфона появится сообщение о том, как вернуть аппарат законному владельцу. С помощью технологии GPS Поиск вы сможете определить, где находится ваш телефон. В ответ на специальное SMS вы получите ссылку с указанием местонахождения смартфона на карте Google Maps. Сменить SIM-карту на украденном смартфоне — первая мысль похитителя. SIM Контроль автоматически заблокирует смартфон при смене SIM-карты и незаметно сообщит настоящему владельцу новый номер телефона.

75.2. Основные функции

- Антивирусная проверка встроенной памяти телефона, а также карт памяти по требованию.
- Проверка всех входящих или модифицируемых объектов без участия пользователя.
- Полная антивирусная проверка по расписанию в удобное для пользователя время.
- Встроенный файервол для ограничения определённых соединений.
- Защита от нежелательных сообщений (спама) и звонков.
- Поиск потерянного или украденного телефона. Вы сможете определить местонахождение пропавшего телефона с помощью функции GPS Поиск. Защита контактов, фото и файлов от попадания в чужие руки. Если ваш смартфон был по-

терян или украден, вы сможете удаленно его заблокировать или стереть на нем все данные. Также вы сможете хранить свои файлы в зашифрованных папках.

- Родительский контроль с функцией GPS Поиск. Вы сможете ограничить звонки и SMS вашего ребенка (например, на платные номера, сервисы «для взрослых» и т.д.). А благодаря функции GPS Поиск вы всегда будете в курсе того, где он находится.
- Личные контакты. Вы можете пометить некоторые контакты или телефонные номера как «личные» — и одним нажатием клавиши скрыть все, что к ним относится (записи в книге контактов, SMS, информацию о звонках). При этом ваш телефон не будет заблокирован — им смогут воспользоваться другие, но они не увидят то, что вы хотели бы сохранить в тайне. Поддерживаются контакты как из памяти телефона, так и с SIM-карты. Доступ к настройке «Личных контактов» защищен паролем. Переход в скрытый режим возможен: вручную, автоматически через заданный период времени, удалённо с помощью специального SMS, отправленного на свой номер.

75.3. Поддержка операционных систем

- Windows Mobile 5.0, 6.0, 6.1, 6.5
- Symbian 9.x Series 60 3rd (только Nokia)
- Android 1.x, 2.x, 4.x

75.4. См. также

- Kaspersky Internet Security
- Антивирус Касперского
- Межсетевой экран

75.5. Ссылки

- Kaspesky Mobile Security на официальном сайте
- Kaspersky Mobile Security 8.0: защита для смартфонов, thg.ru, 27 мая 2009 г
- Kaspersky Mobile Security, itc.ua, 14 октября 2009 г
- Kaspersky Mobile Security 8.0. Первые впечатления, anti-malware.ru, 14 июля 2009 г
- Kaspersky Mobile Security 8.0 защитит смартфоны от кражи, cnews.ru, 27 мая 2009

Глава 76

Malwarebytes' Anti-Malware

Malwarebytes' Anti-Malware (MBAM) — программа, которая находит и удаляет вредоносные программы[1][2]. Производится корпорацией Malwarebytes, была выпущена в январе 2008 года. Она доступна в виде бесплатной версии, которая ищет и удаляет вредоносные программы по ручному запуску, и платной версии, которая обеспечивает сканирование по расписанию, защиту в реальном времени и сканировании флеш-накопителей.

76.1. Замысел

MBAM задумывалась, чтобы находить вредоносные программы, которые другие антивирусы и антишпионы, в основном, не определяют, включая программы, ворующие конфиденциальную информацию, рекламные и шпионские. Однако, программа позволяет обнаруживать, помещать в карантин и удалять трояны и черви. Как выше сказано, программа доступна в бесплатном варианте с неполным функционалом, но также можно купить полную версию программы. Бесплатная версия имеет функции быстрого сканирования и полного сканирования всех дисков. В платной версии доступно мгновенное сканирование оперативной памяти и объектов автозапуска, добавлен защитный модуль, который находится в оперативной памяти и сканирует объекты непосредственно при обращении к ним.

76.2. Доступные языки

MBAM доступна на белорусском, боснийском, болгарском, каталонском, упрощённом китайском, традиционном китайском, хорватском, чешском, датском, голландском, английском, эстонском, финском, французском, немецком, греческом, иврите, венгерском, итальянском, корейском, латышском, македонском, норвежском, польском, португальском, румынском, русском, сербском, словацком, словенском, испанском, шведском и турецком языках.

76.3. В составе программы

- Антивирус
- Антишпионский модуль
- Антируткит
- Блокировщик вредоносных веб-сайтов

76.4. Примечания

[1] pcworld.com (англ.)

[2] cnet.com (англ.)

76.5. Обзоры

- *Хорошевский Алексей.* Обзор Malwarebytes' Anti-Malware (10 апреля 2011). Архивировано из первоисточника 26 мая 2012. (рус.)

Глава 77

Microsoft Anti-Virus for Windows

Майкрософт Анти-Вирус (англ. ***Microsoft Anti-Virus***, **MSAV**) — антивирусное программное обеспечение, представленное Microsoft для собственной операционной системы MS-DOS. Программа впервые появилась в версии MS-DOS 6.0 (1993[1]), последняя версия сопровождала MS-DOS 6.22. В первой версии антивирусной программы не было встроенного механизма обновления (обновления должны были получаться на BBS и вручную устанавливаться пользователем), она была способна распознать 1234 различных вируса[2]. В общем пакете поставлялся также Microsoft Anti-Virus для ОС Windows (*MWAV*), представлявший из себя пользовательский интерфейс, позволявший *MSAV* правильно работать под Windows 3.1.

77.1. История

Microsoft Anti-Virus производился для Microsoft компанией *Central Point Software Inc.* (позднее, в 1994 году, приобретена компанией Symantec и включена в группу по производству программного продукта Norton AntiVirus) и был по существу базовой версией программы Central Point Anti-Virus (*CPAV*), которая, в свою очередь, выпускалась по лицензии компании Carmel Software Engineering (Хайфа, Израиль). *Carmel Software Engineering* продавала тот же продукт под названием *Turbo AntiVirus*, как внутри страны, так и за рубежом.

Microsoft Anti-Virus for Windows также поставлялся компанией *Central Point Software*[3].

77.2. Особенности

MSAV представлял собой стратегию «Найти и удалить» (англ. *Detect and Clean*), был способен проверять загрузочный сектор диска и находить вирусы типа «троянского коня», что соответствовало типичным потребностям пользователей в то время.

Программа также имела возможности для борьбы с вирусами-невидимками (англ. *Anti-Stealth*) и проверки контрольной суммы, что позволяло выявлять любые изменения в имевшихся файлах. Эта технология была предназначена для того, чтобы компенсировать отсутствие регулярных пакетов обновлений. Последнее обновление *MSAV* было выпущено в июне 1996 года[4], оно добавило способность обнаруживать полиморфные вирусы, также была обновлена вирусная база — список обнаруживаемых вирусов был расширен до 2371.

77.2.1. Резидентная программа *VSafe*

VSafe — это резидентный компонент *MSAV*, обеспечивавший защиту от вирусов в реальном времени.

По умолчанию *VSafe* делает следующее:

- проверяет исполняемые файлы на наличие вирусов (в процессе их работы);
- проверяет все диски (жёсткий диск и флоппи) на предмет наличия вирусов в загрузочных секторах;
- предупреждает о попытке вируса произвести запись в загрузочный сектор или таблицу разделов жёсткого диска;
- предупреждает о форматировании, которое может стереть данные с жёсткого диска.

Дополнительные возможности VSafe позволяли:

- предупреждать о попытках исполняемых файлов стать резидентными;
- запрещать программам осуществлять запись на диск;
- предупреждать о попытке записи программой в загрузочный сектор дискеты;
- предупреждать о попытке модифицировать исполняемые файлы.

VSafe имел вирусную базу внутри собственного исполняемого файла, а также был способен загружать дополнительные сигнатуры (обновления) в виде вспомогательного файла.

77.3. Примечания

[1] A History of Microsoft MS-DOS and Windows (and its main competitors) on the 8086 Processor family

[2] List of viruses detectable by MSAV

[3] MS-DOS MSAV command help

[4] Last update MSAV

77.4. См. также

Microsoft Security Essentials

Глава 78

Microsoft Security Essentials

Microsoft Security Essentials (MSE) — бесплатный пакет антивирусных приложений от компании Microsoft, предназначенный обеспечивать борьбу с различными вирусами, шпионскими программами, руткитами и троянскими программами. Данное программное обеспечение работает только на компьютерах, где установлена копия Windows Vista, Windows 7[1][2]), прошедшая валидацию. Антивирус Microsoft Security Essentials пришёл на замену Windows Live OneCare (коммерческая антивирусная программа от Microsoft)[3].

В отличие от Microsoft Forefront, который ориентирован для обеспечения безопасности бизнес-продуктов, Microsoft Security Essentials предназначен для домашнего использования. Кроме того, лицензия позволяет бесплатно использовать MSE не только на домашних компьютерах, но и для малого бизнеса. С октября 2010 года компании могут устанавливать до 10 копий антивируса MSE на свои компьютеры бесплатно[4].

Microsoft Security Essentials получил много положительных отзывов после своего релиза. В июне 2011 года он был самым популярным антивирусным продуктом в Северной Америке и входил в четверку самых популярных антивирусных решений в мире.

Системные требования

78.1. История

23 июня 2009 года была выпущена ограниченная публичная бета-версия продукта, доступная для скачивания только первым 75000 пользователям из США, Израиля и Бразилии. Релиз финальной версии состоялся 29 сентября 2009 года (утром по тихоокеанскому времени). Она была представлена на 19 рынках и доступна на 8 языках. Однако в первый день (29 сентября) из-за технической ошибки пользователи из России не могли скачать и зарегистрировать антивирус. С 16 декабря 2009 года доступна официальная версия для России[5].

19 июля 2010 года Microsoft выпустила Microsoft Security Essentials technical preview 2.0[6].

16 декабря 2010 года вышла официальная вторая версия антивируса, включающая в себя следующие изменения:

- Интеграция с Windows Firewall — в ходе установки Microsoft Security Essentials теперь спрашивает, требуется ли отключить сетевой экран Windows или нет.
- Улучшенная защита от интернет-угроз — MSE теперь интегрирован с Internet Explorer в целях обеспечения защиты от сетевых угроз.
- Новый механизм защиты — обновленный механизм антивирусной защиты обладает улучшенной системой определения сигнатур, новыми возможностями очистки системы от вредоносного ПО, а также предлагает улучшенную производительность.
- Система мониторинга сети — защита от сетевых эксплойтов.

С окончанием 8 апреля 2014 года поддержки Windows XP новые версии MSE на ней больше не работают.

78.2. Функциональность

Функциональность продукта во многом схожа со стандартным Windows Defender, входящим в комплект поставки всех существующих теперь вариантов Windows, но во время инсталляции MSE предшественник, Windows Defender, будет отключен. MSE не включён в состав ОС Windows 7.

Microsoft Security Essentials автоматически проверяет и загружает наличие обновлений вирусных определений, которые публикуются три раза в день в Microsoft Update[7]. Кроме того, пользователи могут скачать обновления вручную из *Microsoft Security Portal*[8].

Используя настройки по умолчанию, архивированные файлы распаковываются, затем сканируются.

Загрузка файлов и электронная почта с вложениями также проверяются. *Служба динамической подписи* (Dynamic Signature Service) пытается лучше определить вредоносные файлы путём проверки обновлений, если приложения ведут себя подозрительно[9]. Прежде чем принять решение по отношению к подозрительному объекту, Microsoft Security Essentials предлагает подсказку для ввода данных пользователю. Если ответ не последует в течение 10 минут, то подозреваемая вредоносная программа обрабатывается согласно правилам по умолчанию. Точки восстановления системы создаются перед удалением вредоносного кода[10]. По умолчанию MSE осуществляет запланированную проверку системы и производит сканирование системы каждое воскресенье в 14:00, но только в то время, когда компьютер находится в режиме ожидания.

Microsoft Security Essentials включает защиту в реальном времени. Является экономной по отношению к оперативной памяти, за сутки использования потребляет не более 4 МБ.

Microsoft Security Essentials является набором продуктов обеспечения безопасности для потребителей, в нём не хватает возможности централизованного управления, которая присутствует в Microsoft Forefront Client Security. MSE включает в себя абсолютно тот же движок защиты против Вредоносных программ (*Microsoft Malware Protection Engine*, сокращёно — *MSMPENG*[11]) и вирусов, который используют и все другие продукты компании Microsoft для защиты десктопных компьютеров против малвари, включая Forefront Client Security, Windows Live OneCare и Windows Defender[12]. MSE не требует регистрации или ввода личной информации, отключает Windows Defender, так как также обеспечивает защиту от шпионского и рекламного ПО[13].

78.3. Лицензия

Уведомление Microsoft Security Essentials о том, что операционная система не является лицензионной копией.

Лицензионное соглашение Microsoft Security Essentials позволяет домашним пользователям загружать, устанавливать и использовать антивирус на неограниченном количестве компьютеров, при условии, что на каждом компьютере будет установлена подлинная копия Microsoft Windows. Малые предприятия также имеют право устанавливать Microsoft Security Essentials для бесплатного использования, но только на 10 компьютеров. Однако, лицензионное соглашение отрицает использование антивируса в учебных заведениях, предприятиях и правительственных органах. Лицензия запрещает пользователям производить реверс-инжиниринг, взлом, декомпиляцию и дизассемблирование Microsoft Security Essentials или публиковать, а также раскрывать результаты тестирования и любые другие оценочные испытания программного продукта третьим лицам без предварительного письменного согласия с корпорацией Microsoft[14].

Microsoft Security Essentials постоянно проверяет валидность операционной системы во время и после установки. Если операционная система не будет распознана как подлинная, то антивирус будет уведомлять пользователя об этом, а затем перестанет функционировать, после определенного периода времени[14].

78.4. Позиционирование

19 ноября 2008 года, после того, как Microsoft публично объявила о Microsoft Security Essentials под кодовым названием Morro, акции компаний Symantec и McAfee резко упали на 9,44 % и 6,62 % соответственно. Эми Барздукас (старший директор по управлению продуктами в *Online Services* и *Windows Division* в Microsoft), объявила о том, что Microsoft Security Essentials не будет напрямую конкурировать с другим платным антивирусным ПО, скорее всего Microsoft позиционирует этот продукт как «Антивирус для 50—60 % пользователей, которые не захотели платить за установку коммерческого антивируса»[15].

Symantec, McAfee и Kaspersky Lab не признали в Microsoft Security Essentials конкурента, утверждая, что антивирус от Microsoft не так хорош, как их собственные[16][17]. Том Поулидж из компании Symantec сказал, что OneCare предлагает неполноценную защиту, а также рассчитан на пользователей, у которых мало опыта, подразумевая, что и Microsoft Security Essentials будет таким же[18]. Джорис Эверс, директор по связям с мировой общественностью из компании McAfee заявил: «С долей рынка OneCare менее чем 2 %, мы прекрасно понимаем решение компании Microsoft переключить своё внимание на свою основную деятельность»[19]. Джастин Пристли из Kaspersky Lab заявил, Microsoft продолжает удерживать низкую рыночную долю на потребительском

рынке, поэтому мы не ожидаем после выхода продукта резкого изменения на игровом поле[19].

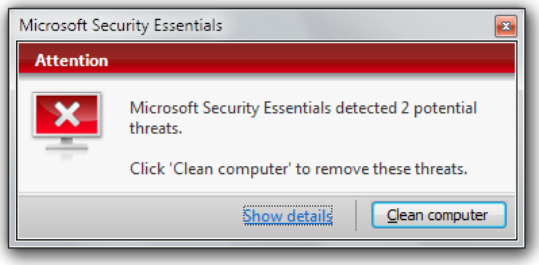
AVG Technologies отнеслась к продукту Microsoft положительно. Представитель компании AVG заявил, что их фирма рассматривает это как позитивный шаг и верит в право на бесплатное антивирусное ПО в течение последних 8 лет. Тем не менее, AVG подняла проблему о распространении ПО и сказала, что Microsoft придётся сделать намного больше, чем просто сделать продукт доступным и бесплатным[19].

AVG Technologies добавила, что интеграция антивируса в Microsoft Windows будет являться нарушением закона в области конкуренции[20]. McAfee и Sophos подтвердили, что антимонопольный иск будет подан, если Microsoft будет поставлять Microsoft Security Essentials вместе с Windows[21].

10 июня 2009 года Microsoft объявила о том, что бета-версия Microsoft Security Essentials будет выпущена в ближайшем будущем, но не указала дату. Далее акции Microsoft выросли на 2,1 %, а акции McAfee и Symantec упали на 0,5 и 1,3 %, соответственно. Дэниел Айвз, аналитик из FBR Capital Markets, сказал, что Microsoft Security Essentials будет долгосрочной конкурентной угрозой, хотя в ближайшем будущем этот скачок будет незначительным[2].

2 октября 2009 года фирма Avast Software выразила двойственное мнение о Microsoft Security Essentials: «MSE не является панацеей, но это также неплохое продолжение OneCare по некоторым утверждениям»[22].

78.5. Некоторые обзоры и награды



Всплывающее уведомление Microsoft Security Essentials о том, что была обнаружена потенциально вредоносная программа.

Первая публичная бета-версия получила несколько положительных отзывов, ссылающихся на низкое потребление ресурсов, простой в использовании пользовательский интерфейс и бесплатность[10][23][24][25]. Брайан Кребс из The Washington Post при тестировании программы обнаружил, что она использует только 4 мегабайта оперативной памяти, даже во время сканирования системы. «Быстрое сканирование» занимает около 10 минут, а «полная» около 45 минут (тест производился в Windows 7)[10].

Обзор Ars Technica дал положительное заключение, ссылаясь на организованный интерфейс, низкий уровень использования ресурсов и на статус freeware[26].

Журнал PC World отметил в Microsoft Security Essentials чёткий и чисто разработанный вкладочный интерфейс пользователя. На первой вкладке указано состояние безопасности системы, другие вкладки позволяют пользователям вручную обновить базу данных, посмотреть журнал и изменить настройки программы. Однако журналисты PC World были озадачены и запутаны некоторыми параметрами антивируса. К примеру, что делать при обнаружении вредоносной программы рекомендуемыми действиями Microsoft Security Essentials, заданными по умолчанию. К рекомендуемым действиям нет никакого описания, за исключением файла справки. Также спутало то, что Microsoft Security Essentials автоматически обновляет себя в интерфейсе. Ко всему прочему, многие считают, что должны вручную обновлять антивирусные базы через вкладку «обновление»[24].

PC Magazine отмечает маленький установочный пакет Microsoft Security Essentials (около 7 МБ, в зависимости от операционной системы), а также быструю скорость установки. С другой стороны, полная установка занимает около 110 МБ дискового пространства, плюс первое обновления заняло от 5 до 15 минут. Редактор также отметил тот факт, что Microsoft Security Essentials устанавливает Windows Update в полностью автоматический режим, который будет автоматически загружать и устанавливать обновления, хотя его можно будет выключить вручную в Панели управления Windows. Установка успешно завершилась на 12 принудительно инфицированных и зараженных машинах. Некоторые «полные» сканирования системы продолжались около часа, а «быстрые» заняли около 35 минут[23].

Хотя стоит заметить, что бета-релиз Microsoft Security Essentials показал себя не очень хорошо при тестах в журнале PC Magazine. Окончательный финальный релиз показал себя лучше в AV-Test.org tests. По словам Нила Рубенкинга, автора PC Magazine, при проверке, которую он провёл в июне 2009 года, Microsoft Security Essentials Beta выявил 89 % вредоносных программ, 30 % кейлогеров, 67 % руткитов и только половину scareware. Защита в реальном времени обнаружила 83 % всех вредоносных программ и заблокировала большинство из них, в этом тесте, MSE нашла 40 % кейлогеров и 78 % руткитов[23] . Позднее, в октябре того же года, AV-Test.org провела серию тестов и испытаний над официальным финальным релизом программного продукта, в которых Microsoft Security Essentials

поймал 98,44 % компьютерных вирусов, червей и троянских программ (545 034 штук), а также 90,95 % spyware и adware (14 222 штук). Также были обнаружены и ликвидированы все 25 испытательных руткитов. Microsoft Security Essentials не дал ложных сигналов[27].

7 января 2010 года Microsoft Security Essentials выиграла в журнале PC Advisor's награду «Best Free Software»[28].

8 июня 2011 года журнал PC Advisor в своём обзоре перечислил антивирус Microsoft Security Essentials 2.0 в списке «Пять лучших бесплатных пакетов безопасности», который также включал в себя Avast! 6 Free Edition, Comodo Antivirus 5.4, AVG Antivirus 2011 и BitDefender Total Security 2012 Beta[29].

78.6. Антивирусный жулик

В феврале 2010 года в Интернете появился ложный пакет безопасности программного обеспечения, называющий себя «Security Essentials 2010».[30][31] Невзирая на сходство названий, по своему внешнему виду эта программа совсем не была похожа на Microsoft Security Essentials. Антивирусное программное обеспечение определяло её как *TrojanDownloader: Win32/Fakeinit*. В ноябре 2010 года данная вредоносная программа появилась снова, на этот раз под названием «Microsoft Security Essentials 2011»[32].

Однако самая опасная форма этих вредоносных программ появилась в октябре 2010 года. Содержащийся в ней вредоносный код был определен и обозначен как *Rogue: Win32/FakePAV*. Эта программа по внешнему виду была весьма подобна Microsoft Security Essentials; она использовала сложную социальную инженерию, чтобы подавить бдительность пользователей и заставить их внедрить вредоносную программу в свои системы, под прикрытием пяти различного рода фальшивых продуктов защиты от вредоносных модулей. После внедрения эта вредоносная программа запрещала запуск и прекращала деятельность 156 различного рода программ, среди которых — редактор реестра, командная строка, Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome и другие веб-браузеры, почтовые клиенты, клиенты мгновенных сообщений, медиапроигрыватели и некоторые развлекательные приложения[33][34][35].

78.7. Ложные срабатывания

Значительный резонанс в средствах массовой информации вызвало ложное срабатывание антивируса на браузер Google Chrome, которое приводило к удалению программы с компьютеров пользователей[36][37]. Эксперт по компьютерной безопасности компании nCircle Security Эндрю Стормз (англ. *Andrew Storms*) заявил, что срабатывание может быть неслучайно, так как браузер от Google стремительно набирает популярность и угрожает рыночной доле Microsoft Internet Explorer[38]. Согласно данным компании Microsoft, выпустившей исправление и принёсшей извинения пользователям, проблема была обнаружена у трёх тысяч человек[39]. Эксперт в области информационных технологий Эдриан Кингсли-Хьюс (англ. *Adrian Kingsley-Hughes*) заявил о том, что будущее внедрение MSE в состав Windows 8 может сделать подобные ложные срабатывания большой проблемой для значительного количества пользователей[40]. Компания Google после случившегося выпустила специальное руководство по восстановлению работоспособности браузера[41], а также обновлённую версию браузера для решения проблем восстановления[42].

78.8. Рыночная доля

Спустя один год после первого выпуска Microsoft Security Essentials, 29 сентября 2010 года, у него появилось более 30 миллионов пользователей[43].

В отчёте *Security Industry Market Share Analysis*, опубликованном в июне 2011 года фирмой «OPSWAT, Inc.», говорится о том, что Microsoft Security Essentials был наиболее популярным антивирусным программным продуктом в мире[44]. Согласно отчёту, у Microsoft Security Essentials было 10,66 % от мирового рынка[44] и 15,68 % рынка Северной Америки[44]. В том же отчёте Microsoft находилась на первом месте в качестве антивирусного вендора в Северной Америке с 17,07 % рыночной доли[44], а также под четвёртым номером антивирусного программного обеспечения во всём мире[44].

Джон Данн из журнала PC World, который проанализировал весь отчёт, отметил, что тенденция к использованию бесплатного антивирусного программного обеспечения — что-то новое. «В конце концов, бесплатные антивирусные пакеты безопасности были вокруг в течение многих последних лет, но, как правило, рассматривались как потенциально скудное отношение по сравнению с платным программным обеспечением.» Он назвал Microsoft Security Essentials, как источник влияния на пользователей ПК принять бесплатное антивирусное программное обеспечение[45].

78.9. Установка

Для установки программы необходимо обладать легальной копией Windows.

Лицензия предусматривает, что в случае нелегальности версии операционной системы последняя будет заблокирована.

С 28 октября 2010 года MSE поставляется как рекомендуемое обновление (KB2267621, позже — KB975959) через Windows Update[46],[47].

Так же программу можно загрузить с официального сайта[48]. Размер установочного файла в зависимости от версии Windows составляет от 7,8 до 9,7 МБ[49].

Системные требования к аппаратному обеспечению к Microsoft Security Essentials могут быть разными, все зависит от операционной системы. Для Windows XP требуется процессор 500 МГЦ и 256 МБ оперативной памяти. Для Windows Vista и Windows 7 антивирус требует процессор 1 ГГц и 1 ГБ оперативной памяти. Также требуется разрешение экрана 800×600 пикселей, 140 МБ свободного пространства и обязательное подключение к Интернету[50].

78.10. Microsoft SpyNet

Microsoft SpyNet является онлайн-сообществом, которое помогает решать пользователям проблемы безопасности, в числе которых как реагировать на потенциальные угрозы, помощь в выборе способа защиты, а также остановки распространение новых инфекций. Пользователи имеют возможность отправлять информационные сведения об обнаруженных вредоносных программах. Подобная информация поможет специалистам создавать новые определения вирусов для наиболее высоконадёжной защиты компьютера.

Информация, которая собирается и отправляется на сервер Microsoft, может быть разная, базовая и расширенная:

- к базовой программе относится информация, в которую включена информация о том, откуда взяты потенциальные угрозы, какие действия пользователей были применены и были ли они успешными.

- к расширенной относится дополнительная информация о вирусах, spyware, потенциально нежелательных программах, включая данные о размещении этих файлов в системе пользователя, их имена, работе и влиянии на систему. В некоторых случаях личные данные могут быть отправлены принудительно на сервер Microsoft, но сама корпорация не использует эти сведения для идентификации пользователя и связи с ним.[51]

78.11. Примечания

[1] Microsoft Security Essentials is now Final. Microsoft Corporation (1 October 2009). — «It is available for XP x86, Vista/Windows 7 x86 & x64» Проверено 8 ноября 2009. Архивировано из первоисточника 2 апреля 2012.

[2] *Finkle, Jim* Update 3-Microsoft will soon unveil free antivirus software. Thomson Reuters (10 June 2009). Проверено 4 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[3] *Thurrott, Paul* Microsoft Security Essentials Public Beta. *Paul Thurrott's SuperSite for Windows* (18 June 2009). Проверено 4 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[4] Free Microsoft Security Essentials Coming for Small Businesses (рус.). Microsoft. Проверено 23 сентября 2010. Архивировано из первоисточника 2 апреля 2012.

[5] Microsoft Security Essentials доступен для России

[6] *LeBlanc, Brandon* Beta for Next Version of Microsoft Security Essentials Now Available. *The Windows Blog*. Microsoft Corporation (20 July 2010). Проверено 21 июля 2010. Архивировано из первоисточника 2 апреля 2012.

[7] *Mills, Elinor* Microsoft's free antimalware beta on the way. CNET (18 June 2009). Проверено 10 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[8] Install the latest Microsoft Security Essentials definition updates. Microsoft Corporation (11 March 2010). Проверено 15 марта 2010. Архивировано из первоисточника 2 апреля 2012.

[9] *Hoffman, Stefanie* Microsoft Security Essentials Beta Reaches Max Downloads. ChannelWeb (24 June 2009). Проверено 19 июля 2009. Архивировано из первоисточника 18 августа 2012.

[10] *Krebs, Brian* Microsoft Debuts Free Antivirus Software Beta. The Washington Post (24 June 2009). Проверено 10 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[11] *Ševeček, Ondřej* Microsoft Security Essentials. *TechNet Blog CZ/SK*. Microsoft Corporation (4 November 2009). — «V případě souboru ze sítě je to poněkud zajímavější. Soubory ze sítě musí být nejprve zkopírovány na lokální počítač a teprve zde je skenován službou Microsoft Antimalware Service (MSMPENG.EXE). [*In the case of the file from the network, it's a little more interesting. Files from the network must first be copied to the local computer, and only here is scanned by the Microsoft Antimalware Service (MSMPENG).*]» Проверено 16 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[12] Microsoft Security Essentials (MSE) released. *TechNet Edge*. Microsoft Corporation (29 September 2009). Проверено 16 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[13] *Bott, Ed* How good is Microsoft's free antivirus software?. ZDnet (18 June 2009). Проверено 6 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[14] MICROSOFT SOFTWARE LICENSE TERMS. *Microsoft Security Essentials web site*. Microsoft Corporation (22 September 2010). Проверено 8 октября 2010. Архивировано из первоисточника 2 апреля 2012.

[15] Позиционирование программы

[16] *Messmer, Ellen* Anti-malware test in hand, Symantec swats Microsoft Security Essentials. ITworld (www.itworld.com) (1 October 2009). Проверено 21 июля 2010. Архивировано из первоисточника 2 апреля 2012.

[17] *Keizer, Gregg* Rivals mock Microsoft's free security software. Computerworld (29 September 2009). Проверено 30 сентября 2009. Архивировано из первоисточника 2 апреля 2012.

[18] Security 'hippos' dismiss Microsoft Morro launch, *Guardian.co.uk*, *Guardian News and Media Limited* (27 November 2008). Проверено 16 декабря 2010.

[19] *Vamosi, Robert* Antivirus firms shrug at Microsoft's free security suite. CNET (19 November 2008). Проверено 6 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[20] *Fried, Ina* Will Microsoft's antivirus move draw antitrust fire?. CNET (18 November 2008). Проверено 6 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[21] *Schofield, Jack*. Waiting for Morro: Microsoft's free anti-virus software, *Guardian.co.uk*, *Guardian News and Media Limited* (11 June 2009). Проверено 6 июля 2009.

[22] *Steckler, Vincent* And what about Microsoft Security Essentials—MSE?. *avast! blog*. Avast Software a.s (2 October 2009). Проверено 20 сентября 2010. Архивировано из первоисточника 2 апреля 2012.

[23] *Rubenking, Neil J.* Microsoft Security Essentials beta. PC Magazine (18 June 2009). Проверено 10 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[24] *Mediati, Nick* Microsoft Security Essentials: Basic, Automatic Protection. PC World (24 June 2009). Проверено 10 июля 2009. Архивировано из первоисточника 2 апреля 2012.

[25] *Angad, Ulhas M.* Microsoft Security Essentials Review. Satishsays.com (17 October 2009). Проверено 8 октября 2009. Архивировано из первоисточника 2 апреля 2012.

[26] *Protalinski, Emil* First look: Microsoft Security Essentials impresses. Ars Technica (29 September 2009). Проверено 30 сентября 2009. Архивировано из первоисточника 2 апреля 2012.

[27] *Whitney, Lance*. Security Essentials fares well in AV-Test trial, *CBS Interactive* (2 October 2009). Проверено 24 июля 2010.

[28] Microsoft wins PC Advisor's Best Free Software award — PC Advisor Awards 2010: winners announced. PC Advisor (7 January 2010). Проверено 1 августа 2010. Архивировано из первоисточника 2 апреля 2012.

[29] Five of the best free security suites, *IDG* (8 June 11). Проверено 12 июня 2011.

[30] If it calls itself "Security Essentials 2010", then it's possibly fake, innit?. *Microsoft Malware Protection Center blog*. Microsoft Corporation (24 February 2010). Проверено 1 марта 2010. Архивировано из первоисточника 2 апреля 2012.

[31] Encyclopedia Entry: TrojanDownloader:Win32/Fakeinit. *Malware Protection Center*. Microsoft Corporation (2 April 2009). Проверено 18 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[32] New Year, Same Old Rogues. *Microsoft Malware Protection Center blog*. Microsoft Corporation (15 November 2010). Проверено 18 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[33] Fake Microsoft Security Essentials software on the loose. Don't be fooled by it!. *Windows Security Blog*. Microsoft Corporation (25 October 2010). Проверено 18 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[34] MSRT Tackles Fake Microsoft Security Essentials. *Microsoft Malware Protection Center Blog*. Microsoft Corporation (9 November 2010). Проверено 18 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[35] Encyclopedia Entry: Rogue:Win32/FakePAV. *Malware Protection Center*. Microsoft Corporation (9 November 2009). Проверено 18 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[36] *Ed Bott.* Users report Microsoft Security Essentials removes Google Chrome (англ.). ZDNet (30 September 2011). Проверено 1 октября 2011. Архивировано из первоисточника 2 апреля 2012.

[37] *Dan Goodin.* Pandemonium as Microsoft AV nukes Chrome browser (англ.). The Register (30 September 2011). Проверено 1 октября 2011. Архивировано из первоисточника 2 апреля 2012.

[38] *Gregg Keizer.* Microsoft kills Google Chrome with bad malware signature (англ.). Computerworld (30 September 2011). — «"Wow, that's certainly one way to win the browser war," said Andrew Storms, director of security operations at nCircle Security. Storms was referring to the battle between Microsoft's Internet Explorer (IE) and rivals, including Chrome, for usage share. According to data from one Web metrics firm, Chrome will pass Mozilla's Firefox as the second-most-popular browser by the end of this year, pitting Google and Microsoft for the top spot.» Проверено 1 октября 2011. Архивировано из первоисточника 2 апреля 2012.

[39] Research PWS:Win32/Zbot (англ.). Microsoft. Проверено 1 октября 2011. Архивировано из первоисточника 2 апреля 2012.

[40] *Adrian Kingsley-Hughes.* Do you STILL trust Microsoft to build antivirus support into Windows 8? (англ.). ZDNet (1 October 2011). Проверено 1 октября 2011. Архивировано из первоисточника 2 апреля 2012.

[41] *Mark Larson.* Problems with Microsoft Security Essentials (англ.). Google (30 September 2011). Проверено 1 октября 2011. Архивировано из первоисточника 2 апреля 2012.

[42] *Jason Kersey.* Stable and Beta Channel Updates (англ.). Coogle (1 October 2011). Проверено 1 октября 2011. Архивировано из первоисточника 2 апреля 2012.

[43] Microsoft Security Essentials racks up 30 million users. TechRadar (29 September 2010). Проверено 30 марта 2011. Архивировано из первоисточника 2 апреля 2012.

[44] Security Industry Market Share Analysis – June 2011 (PDF). *OPSWAT Market Share Report*. OPSWAT (6 June 2011). Проверено 12 июня 2011. Архивировано из первоисточника 2 апреля 2012.

[45] *Dunn, John E.*. Free Antivirus Programs Rise in Popularity, New Survey Shows (7 June 2011). Проверено 12 июня 2011.

[46] Microsoft Security Essentials is offered as an optional update

[47] Microsoft Security Essentials Offered via Windows Update

[48] Официальный сайт MSE

[49] Download Details: Microsoft Security Essentials. *Microsoft Download Center*. Microsoft Corporation (16 December 2010). Проверено 16 декабря 2010. Архивировано из первоисточника 2 апреля 2012.

[50] Find out what you need to know about installing and running Microsoft Security Essentials. Microsoft Corporations. Проверено 29 сентября 2009. Архивировано из первоисточника 2 апреля 2012.

[51] Microsoft Security Essentials — What is the Microsoft SpyNet Community?

78.12. Ссылки

- **microsoft.com/security_essentials** — официальный сайт Microsoft Security Essentials (рус.)
- Обзор возможностей, установка, настройка
- Обзор Microsoft Security Essentials 2.0 — бесплатный антивирус для Windows — Обзоры — Статьи — Anti-Malware.ru

Глава 79

NANO Антивирус

«NANO Антивирус» (англ. *NANO Antivirus*) — российская антивирусная программа, предназначенная для защиты компьютера от всех видов вредоносного программного обеспечения: вирусов, троянских программ, червей и прочих опасных программ. Разрабатывается компанией «НАНО Секьюрити».

79.1. Описание

Разработчики позиционируют NANO Антивирус как высокотехнологичный продукт, гарантирующий надёжную защиту компьютера от любых видов вирусов, троянских программ, червей и прочего вредоносного программного обеспечения, а также безопасную работу в сети Интернет.

NANO Антивирус использует перспективные методы разработки в области защиты информации. Благодаря технологии глубокой эмуляции антивирус позволяет обнаруживать и лечить даже самые сложные полиморфные и зашифрованные вирусы. Имеет функцию достаточно сильной поддержки инструментов для распаковки и работы с архивами, обеспечивающую определение различных вредоносных программ, заархивированых другими программами, что в свою очередь предоставляет защиту от повторных заражений, вызванных одними и теми же перепакованными объектами.

Антивирус предусматривает поддержку расписания, то есть выполнение сканирования системы и обновления в установленный промежуток времени. Подобные задачи позволяют автоматизировать конкретные действия для предоставления максимальной защиты данных. NANO Антивирус производит полное сканирование системы, переносного носителя информации, обновление антивирусной базы данных или компонентов просто и удобно для пользователя.

NANO Антивирус предоставляет безопасность в режиме реального времени. Если эта функция включена, то абсолютно все файлы, к которым идет доступ, независимо, системой или пользователем, незамедлительно проверяются на наличие зловредного кода. В список исключений, иначе называемый «доверенная зона», можно добавить любой объект, следовательно, внесённые в список данные не проверяются при сканировании файлов. Подобный метод позволяет пользователям создать зону доверенных файлов, в безопасности которых есть уверенность, и сэкономить время, которое тратится на обработку больших архивов с данными.

Как и во многих других антивирусах, в NANO Антивирус есть функция карантина, служащая для изоляции всех подозрительных файлов в системе. Файлы из карантина можно отправлять в службу технической поддержки для более глубокого анализа и добавления в вирусную базу при необходимости.

Для тех, кто обладает административными правами, реализована функция запуска от имени другого пользователя. Поддерживается защита от смены настроек; при включенной функции изменить настройки можно только с помощью пароля. Есть возможность автоматического копирования (зеркалирования) обновлений в указанную пользователем папку, которая может быть настроена для использования в качестве источника обновлений. Эти функции полезны для удобной интеграции комплекса в инфраструктуру.

NANO Антивирус обладает простым в управлении графическим интерфейсом и оптимизирован для быстрого запуска, а также на минимальную нагрузку на ресурсы системы. Одной из самых отличительных характеристик в настройке интерфейса антивируса является то, что можно выбрать и настроить конкретно требуемый набор каких-либо функциональных возможностей. Те пользователи, которые не испытывают необходимость в дополнительных параметрах защиты данных, могут выбрать более облегчённый вариант внешнего вида программы с наиболее оптимальными настройками. Подобные действия позволяют в кратчайшие сроки задать надёжную и эффективную защиту персональных данных на компьютере, тем самым не тратя времени на выполнение тонкой настройки. Для других, более опытных пользователей, к примеру, программистов или администраторов, существуют более углублённые и сложные настройки интерфейса антивируса, дающие возможность использовать более широкие возмож-

ности программы для самых разнообразных задач.

Весь механизм антивируса оптимизирован так, что ресурсы системы расходуются в минимальном количестве, обеспечивая комфортную работу, не вызывающую проблем с другими приложениями и процессами, запущенными в операционной системе, при проверке файлов на наличие вирусов.

79.2. Функциональность

- Защита от всех видов вредоносного программного обеспечения, включая шифрованные и полиморфные разновидности.
- Защита системы в режиме реального времени.
- Расширенная поддержка средств распаковки.
- Эвристический анализ.
- Возможность создания пользовательских задач сканирования и обновления.
- Многопользовательский режим.
- Автоматическое обновление вирусных баз.
- Зеркалирование обновлений.
- Возможность выбора интерфейса программы.
- Английская и русская локализация интерфейса, переключаемая «на лету».
- Автоматическая проверка сменных носителей при подключении.

79.3. Распространение

NANO Антивирус (бета) распространяется бесплатно, скачать установочный файл можно на официальном сайте программы[3]. NANO Антивирус (бета) полностью бесплатен для всех категорий пользователей и организаций, в том числе для коммерческих организаций, а также для школ, ВУЗов и других учебных заведений. По запросу на e-mail службы технической поддержки бесплатно предоставляется файл лицензии, предназначенный для установки на любое количество рабочих мест[4].

79.4. Поддельный NANO Antivirus

После выхода антивируса в сети Интернет появилась вредоносная программа, определявшаяся как Trojan.Binary.Win32.FakeAlert.nano. Её основная задача заключается в том, чтобы ввести пользователя в заблуждение и, после сканирования системы, вывести ложные результаты с якобы инфицированными данными на компьютере. После сообщения, троян предлагал пользователю приобрести антивирусную программу, которая позволила бы оперативно удалить найденные угрозы в системе.

Троян Trojan.Binary.Win32.FakeAlert.nano был обнаружен сотрудниками NANO Security следующим образом: на подставных (заражённых) веб-сайтах выскакивало всплывающее окно с информацией, что на компьютере пользователя обнаружены вирусы. В случае если доверчивый пользователь щёлкал мышью по сообщению, происходила переадресация на фишинговую страницу, которая имитировала онлайн-антивирусный сканер, который также выводил ложные данные об обнаружении вредоносной программы и рекомендовал установить «антивирус» на компьютер. После установки «антивирус» записывал себя во все возможные секции автозапуска системы и производил сканирование с выводом ложных сведений.[5]

79.5. Системные требования

- Процессор 1,2 ГГц и выше (рекомендуется 2 ГГц и выше).
- ОЗУ 512 МБ для Windows XP (рекомендуется 1 Гб и выше).
- ОЗУ 1 Гб для Windows Vista и более новых ОС Windows (рекомендуется 2 Гб и выше).
- Операционная система Windows XP SP3 и выше (рекомендуется Windows 7 и более новые ОС).

79.6. Сертификация

79.6.1. OPSWAT Inc.

В марте 2011 года NANO Антивирус успешно прошёл сертификацию OPSWAT (бывший OESIS OK) в категории «Антивирусы». В ходе процесса тестирования было показано, что NANO Антивирус:

- имеет полную совместимость с OESIS Framework;
- не содержит внутри программы компоненты с вредоносными объектами;
- работает со всеми операционными системами Microsoft Windows, которые были заявлены разработчиками[6].

По результатам сертификации NANO Антивирус стал сертифицированным партнером компании OPSWAT. [7]

79.6.2. Intel®

В октябре 2012 года NANO Антивирус был протестирован с помощью специального программного обеспечения, предоставленного компанией Intel®. По результатам тестирования было установлено, что NANO Антивирус обеспечивает ускорение работы в 3,51 раз на 4-ядерных системах по сравнению с одноядерными. По этому показателю, согласно статистике Intel®, NANO Антивирус вошел в 27 % лучших программ из всех, протестированных подобным образом, и получил официальный статус Enhanced for Intel® Inside® Core™. Также компания NANO Security получила статус партнера компании Intel® в категории Software Premier Elite Partner.

79.6.3. 1C

12 января 2015 года NANO Антивирус получил очередной сертификат «1С:Совместимо» от компании 1С[8]. Сертификат подтверждает, что NANO Антивирус обеспечивает сохранность данных в среде «1С:Предприятие», осуществляя проверку в реальном времени всех объектов, к которым производится доступ пользователем или системой. Сертификат действителен до 12.01.2017 года.

79.7. Участие в онлайн-сканерах проверки файлов

NANO Антивирус принимает участие в следующих онлайн-сканерах: VirusTotal[9], Metascan Online[10], Infovirus[11].

79.8. Сопутствующие продукты

79.8.1. Онлайн-сканер NANO Антивирус

Бесплатный сервис облачной проверки подозрительных файлов. Позволяет проверять файлы размером до 20 Мб.

79.8.2. NANO Antivirus Sky Scan

Бесплатное приложение Магазина Windows. NANO Antivirus Sky Scan позволяет отправлять подозрительные файлы на проверку сервисом онлайн-сканирования NANO Антивирус. Также служит инструментом управления и быстрого доступа к установленному на устройстве пользователя NANO Антивирусу.

NANO Antivirus Sky Scan предназначен для ОС Windows 8, Windows 8.1 и Windows 10.

79.9. Интересные факты

- Компания «НАНО Секьюрити» является выпускником программы BizSpark корпорации Microsoft. Дата выпуска — 18 августа 2012 г.[12]

79.10. Примечания

[1] Выложена бета-версия NANO Антивирус!

[2] Состоялся выход финальной версии NANO Антивируса Pro!

[3] «NANO Антивирус»: официальный сайт

[4] Частые вопросы о NANO Антивирус и ответы на них

[5] Осторожно, подделка! Троян, имитирующий антивирус.

[6] Список продуктов, сертифицированных OPSWAT

[7] Сертифицированные партнеры компании OPSWAT

[8] Новости компании «1С»

[9] VirusTotal

[10] Metascan Online

[11] Infovirus

[12] Партнеры «НАНО Секьюрити» — Microsoft BizSpark

79.11. Ссылки

- Официальный сайт «NANO Антивирус» (англ.) (рус.)
- Список антивирусных вендоров на сайте тестовой лаборатории AV-Comparatives
- «NANO Антивирус» в списке «Лучший софт 2010 года» по версии журнала *Hard'n'Soft*
- «NANO Антивирус» в новостях журнала *Hard'n'Soft*
- *Крупин, Андрей.* NANO Антивирус 0.8.0.7 beta: защита компьютера от вредоносного ПО. 3DNews (23 мая 2010).
- *Крупин, Андрей.* NANO Антивирус 0.12.0.0 beta: защита ПК от цифровых угроз. 3DNews (11 сентября 2010).
- Обзор антивирусов под WINDOWS на компьютерном форуме *Ru-Board*

- NANO Антивирус 0.12.0.0 Beta на *securitylab.ru*
- Бета-версия нового антивируса под названием NANO Антивирус. iXBT (7 июля 2011). Архивировано из первоисточника 1 августа 2012.

Глава 80

Norton AntiVirus

Norton AntiVirus — антивирусная программа. Производится американской компанией Symantec на протяжении десяти лет. Последняя версия вышла в 2014 году.

80.1. Основные технологии

- Защита от вирусов
- Защита от программ-шпионов
- Защита от руткитов
- Импульсные обновления
- Защита от ботов
- Карта и мониторинг сети
- Norton Reputation Service
- Эвристическая защита SONAR 3

80.2. Системные требования

Поддерживаемые операционные системы:

- Microsoft Windows XP (32-разрядные версии) Home Edition/Professional/Tablet PC/Media Center
- Microsoft Windows Vista (32- или 64-разрядные версии) Starter/Home Basic/Home Premium/Business/Ultimate
- Microsoft Windows 7 (32- и 64-разрядные версии) Начальная/Домашняя базовая/Домашняя расширенная/Максимальная
- Microsoft Windows 8 (32- и 64-разрядные версии)

Аппаратные требования:

- Процессор 300 МГц для Microsoft Windows XP, 1 ГГц для Microsoft Windows Vista/Windows 7/Windows 8.
- Оперативная память — 256 Мб.
- Свободная память на компьютере — 300 Мб.
- Привод для CD/DVD (если установка осуществляется с компакт-диска).

Поддержка браузеров:

- Microsoft Internet Explorer 6.0 и более новые версии (только 32-разрядные версии).
- Mozilla Firefox 3.0 и более новые версии (только 32-разрядные версии).

Сканирование электронной почты поддерживается для клиентов POP3

80.3. Примечания

80.4. Ссылки

- **norton.com** — официальный сайт Norton AntiVirus

Глава 81

Outpost Antivirus

Outpost Antivirus — антивирус от российской компании Agnitum. Первоначально антивирус поставлялся в комплекте с Outpost Security Suite, но 2 марта 2008 года[1] был представлен в качестве отдельного продукта на «Вернисаже 1С» и 12 марта[2] был представлен пользователям и готов к продаже.
Антивирусный компонент в последних версиях Outpost 7.5 включает в себя новейшие технологии по защите от вредоносного ПО, которые обеспечивают безопасный веб-сёрфинг и сохранность данных компьютера, не мешая ежедневной работе пользователя. Оптимизируя скорость сканирования на вирусы и снижая системные и аппаратные требования Outpost для удобства работы на ограниченных в ресурсах ПК и нетбуках, разработчики Agnitum от версии к версии делают защиту Outpost ещё более легкой и нетребовательной.

81.1. Возможности

- Антишпион.
- Проактивная защита.
- Защита интернет-соединения.
- Защита личной информации.
- Защита электронной почты.
- Блокировка «опасного» контента на веб-страницах в Internet Explorer (специальная вкладка).
- Фильтр рекламы (для всех браузеров, начиная с версии 2009).
- Поддержка ОС Windows 8.
- Технология **SmartDecision**, осуществляющая статический анализ запускаемых файлов, на основе множества критериев оценивает потенциальную угрозу и выводит подсказку пользователю о дальнейших действиях.
- **ImproveNet** — «облачный» сервис, собирающий информацию о локальном взаимодействии приложений на компьютере. Эти новые правила автоматически обновляются у подписчиков ImproveNet и используются для различения вредоносной и безопасной активности.
- SmartScan (кэширование статуса проверки) — технология, повышающая скорость проверки компьютера на наличие вредоносных объектов путем создания специальной базы, в которой хранится информация о уже проверенных «чистых» файлах, которые исключаются из проверки.

81.2. Профессиональное признание

Благодаря совместным усилиям двух независимых антивирусных лабораторий, работающих над созданием и обновлением современной и многогранной базы вирусных сигнатур, антивирусные решения Outpost находятся среди лидеров по уровню обнаружения широкого распространенного (in-the-wild) вредоносного ПО. Outpost последовательно (в июне, августе, октябре и декабре 2010 г.) получал награды VB100 британского журнала VirusBulletin, подтверждая соответствие современным стандартам антивирусной защиты для 32-битных и 64-битных операционных систем Windows. Другие признанные организации также отмечали высокий уровень обнаружения вредоносного ПО антивирусными решениями Outpost. Кроме того, Matousec.com и Anti-malware.ru, известные тестовые площадки, исследующие производительность и надежность продуктов Интернет-безопасности, высоко оценивают уровень самозащиты и проактивной защиты решений Outpost.

81.3. Награды

- 25-08-2011 комплексный продукт по безопасности компании Agnitum получил восьмую подряд

награду VB100 со 100 % обнаружением самых распространенных вредоносных программ и полиморфных вирусов.

- Компания Agnitum вошла в число 5 производителей антивирусов, получивших все сертификации VB100 подряд на ОС Windows (Windows 2000, Windows XP, Vista, Server 2003/2008, Windows 7) с начала 2010 года. Общее число непрерывно пройденных сертификаций VB100% для Outpost составляет более 10.
- 10-05-2012 антивирусы от Agnitum уже 11 раз подряд за 2 года сертифицируются для Windows.
- 18-07-2012 по результатам тестирования, проведенного независимой лабораторией Virus Bulletin, антивирусы от Agnitum получили 12 раз подряд награду VB100 http://www.agnitum.ru/news/2012-07-18-oss-vb100-windows-server-2008.php

81.4. Примечания

[1] Agnitum представила Outpost Antivirus Pro 2008 на Вернисаже 1С в Москве

[2] Agnitum выпускает Outpost Antivirus Pro — новый проактивный антивирус по цене обновлений

81.5. Ссылки

- http://www.agnitum.ru/
- Outpost 7.5: Технология SmartDecision
- Outpost 7.5 Антивирус + Антишпион

Глава 82

Panda Security

Panda Security SL, прежде **Panda Software** — компания, работающая в сфере компьютерной безопасности, основана в 1990 году бывшим руководителем Panda Микелем Уризарбаррена (Mikel Urizarbarrena) в городе Бильбао, Испания. Первоначально компания была ориентирована на производство антивирусного программного обеспечения, впоследствии она расширила линейку своих продуктов за счет приложений, включающих в себя файервол, приложений по обнаружению спама и шпионского ПО, технологии по предотвращению кибер-преступлений, а также других систем управления и утилит безопасности для домашних и корпоративных пользователей.

Продукты Panda содержат средства безопасности для домашних и корпоративных пользователей, включая защиту от кибер-преступников и различных видов вредоносных программ, которые способны нанести вред IT-системам, например, спам, хакеры, шпионы, дозвонщики и нежелательный веб-контент, также как и обнаружение WiFi-вторжений. Ее зарегистрированная технология под названием TruPrevent представляет собой набор проактивных инструментов, предназначенных для блокировки неизвестных вирусов и вторжений. В 2007 году Panda выпустила новую модель безопасности под фирменным названием Collective Intelligence[1], которая использует технологии grid computing для сбора и обнаружении вредоносных программ.

Недавно Panda представила на рынке новые решения[2], предоставляющие безопасность «из облака» благодаря своей запатентованной технологии Коллективный разум (Collective Intelligence), которая представляет собой автоматизированную систему сканирования, классификации и дезинфекции для борьбы с новыми IT-угрозами.

82.1. О компании

82.1.1. Обзор

В 2005 году Panda Security была четвёртым в мире производителем антивирусных решений с долей рынка 3,2 %.[3] Компания, которая раньше на 100 % принадлежала Уризарбаррена (Urizarbarrena), 24 Апреля, 2007 года анонсировала продажу 75%-ной доли Южно-Европейской инвестиционной группе Investindustrial и частной компании Gala Capital.[4] 30 июля, 2007 года компания изменила своё название с Panda Software на Panda Security, а Уризарбаррена (Urizarbarrena) передал управление Хорхе Динаресу Jorge Dinares. Спустя год, 3 июня 2008 года, совет директоров проголосовал за снятие с должности Динареса (Dinares) и назначение на его пост Хуана Сантану (Juan Santana), занимавший на тот момент должность CFO.[5][6]

Начиная с 1997 года, компания присутствует в списке 500 наиболее быстро растущих компаний Европы. Panda Software является лидером рынка в Испании и в 1998 году стала лидирующим европейским разработчиком антивирусного программного обеспечения. В 2003 году Panda Software достигла 1000%-ного роста доходов в мире.

Panda Software имеет клиентов в более чем 200 странах мира, её офисы расположены в более 50 странах мира, включая Уругвай, США, Канаду, Германию, Китай, Великобританию, Францию, Таиланд, Грецию, Финляндию, Данию, Швецию, Норвегию, Перу, Болгарию, Пакистан, Польшу, Турцию, Словакию, Словению и Швейцарию. В 2003 году Panda Software открыла свои представительства в Японии, Аргентине, Корее и Австралии.

Panda Security оценивается аналитиками Gartner в качестве технологического инноватора.[7] Среди технологических вех компании следует отметить, что она первой выпустила системы безопасности, основанные на концепции SaaS (Security as a Service), или антивирусные решения, которые предоставляют защиту «из облака» (cloud computing). Они основаны на модели безопасности, называемой в Panda Коллективным разумом (Collective Intelligence), представленной на рынке в 2007[8] году[8]

По словам CEO компании, основное преимущество, которое предоставляет данная модель безопасности, заключается в том, что она позволяет автоматизировать процессы сканирования угроз вме-

сто ручного сканирования, применяемого другими компаниями[9]], делая быстрее и более эффективными процессы обнаружения вредоносных программ.

Panda Security имеет филиалы в США, Германии, Австрии, Бельгии, Нидерландах, Франции, Великобритании, Швеции, Испании и Японии. В дополнение к этому, компания имеет свои представительства, работающие по франшизе, в 44 странах мира, а также клиентов, расположенных в 200 странах мира.

Panda Security в антивирусной индустрии конкурирует со многими компаниями, среди которых следует отметить Symantec Corp, Лаборатория Касперского, McAfee Inc и Trend Micro Inc.

82.2. Продукты

82.2.1. Бесплатные продукты

- Panda Cloud Antivirus FREE — бесплатный «облачный» антивирус, предназначенный для защиты от вирусов, шпионов, руткитов и рекламного ПО[10] (на ранней бета-стадии). Panda Cloud Antivirus работает на основе Коллективного разума — системы, которая значительно увеличивает уровень обнаружения, не влияя на производительность компьютера.

Коллективный разум работает в качестве огромной онлайновой базы данных, которая хранит и классифицирует информацию, необходимую для обнаружения угроз в режиме реального времени. Эта база данных постоянно обновлена благодаря информации, которая поступает от миллионов пользователей сообщества Panda Security во всём мире — отсюда и название системы «Коллективный разум». Вследствие этого для более тщательной проверки на наличие вирусов, и т. д. компьютер должен быть подключен к интернету.

- Panda Antirootkit
- Panda USB Vaccine

82.2.2. Домашние продукты

- Panda Antivirus Pro 2012 (содержит: антивирус, антишпион, антифишинг, антируткит, файервол)
- Panda Internet Security 2012 (содержит: антивирус, антишпион, антифишинг, антируткит, файервол, антиспам, родительский контроль)
- Panda Global Protection 2012 (содержит: антивирус, антишпион, антифишинг, антируткит, файервол, антиспам, родительский контроль, оптимизацию работы системы, резервирование данных backup)
- Panda Antivirus for Netbooks (содержит: антивирус, антишпион, антифишинг, антируткит, файервол)
- Panda ActiveScan 2.0
- Panda Security for Linux

82.2.3. Корпоративные продукты

- Panda Security for Business
- Panda Managed Office Protection
- Panda Managed E-mail Protection
- Panda Malware Radar (бесплатный)

82.2.4. Сетевые устройства

- GateDefender Performa
- GateDefender Integra

82.3. Технологии TruPrevent

TruPrevent, которая была анонсирована в 2003 году, является набором технологий, разработанных компанией Panda Security для проактивной защиты домашних и корпоративных компьютеров, в противоположность традиционным антивирусным продуктам, которые предоставляют реактивную защиту.

Технологии Truprevent предлагают генетическую защиту от многих угроз, в большинстве своем применяющихся для создания новых вредоносных программ, а также политики и правила, разработанные на основе новых уязвимостей, которые появляются каждый день.

Благодаря огромному количеству новых вредоносных программ, которые появляются ежедневно, в 2007 году лаборатория PandaLabs обнаружила в среднем за день 3000 новых образцов,[11] а в 2009 году это значение увеличилось до 35000, Panda Security решила разработать систему защиты, которая смогла бы автоматически обнаруживать, сканировать и классифицировать вредоносные программы в режиме реального времени. Эта модель безопасности, презентованная в 2007 году, была названа «Коллективный разум (Collective Intelligence)», и она является базисом для новых решений, которые предлагают безопасность «из облака».

Данная технология была внедрена в антивирусные продукты 2009 и 2010 для домашних пользователей,

а также в новый продукт Panda Cloud Antivirus, который компания назвала первым в истории антивирусом, предоставляющим защиту «из облака»[12]

Эти антивирусные продукты содержат только информацию об образцах вредоносных программ, которые являются причиной большинства инфекций в настоящее время, в то время как остальная информация хранится в базе знаний Panda. Антивирус при необходимости подключается к этой базе знаний. Данная система разработана для того, чтобы предлагать в режиме реального времени защиту от тысяч образцов новых вредоносных программ, использование же базы знаний всего сообщества пользователей позволяет предлагать дополнительную защиту и значительно снизить использование ресурсов компьютера.[13]

82.4. См. также

- Panda Cloud Antivirus

82.5. Примечания

[1] Можно перевести как «коллективный разум»

[2] Review: Panda Cloud Antivirus — Security

[3] Gartner Says Worldwide Antivirus Software Market Increased 13.6 Percent in 2005

[4] Investindustrial and Gala Capital invest in Panda Software to undertake an important expansion plan and launch new IT security solutions globally

[5] Panda Security

[6] Jorge Dinares: new CEO of the Panda Software Group

[7] Panda Security positioned in «visionaries» quadrant of magic quadrant for Enpoint Protection Platforms

[8] Collective Intelligence — Antivirus — PANDA SECURITY

[9] against increasing malware in recession times

[10] Panda Cloud Antivirus FREE

[11] number of new strains of malware that appeared in 2007 increased tenfold with respect to the previous year

[12] Security launches its 2009 products, the first antivirus in history to use Collective Intelligence and protect from the cloud

[13] Collective Intelligence works and security from the cloud works

82.6. Ссылки

- Panda Security Homepage
- ActiveScan 2.0 — бесплатный online сканер
- Panda Corporate Products Homepage
- Panda Research Blog
- PandaLabs Blog

Глава 83

Qihoo 360 Antivirus

Qihoo 360 Antivirus — бесплатный антивирус с 4 антивирусными движками: Avira AntiVir, Bitdefender, QVM II и облачный 360 Cloud. Включает проактивную защиту, веб-защиту от вредоносных сайтов и загрузок, анти-кейлоггер. Есть версия для Андроид[1]

83.1. Особенности Qihoo 360 Antivirus

Антивирус существует в двух версиях: 360 Total Security и 360 Total Security Essential (бывший 360 Internet Security). Антивирус использует сигнатурные, проактивные и облачные технологии.

Qihoo 360 включает защиту в режиме реального времени с помощью четырех антивирусных движков: Avira AntiVir, Bitdefender с эффективным уровнем обнаружения, проактивный QVM II для защиты от новейших угроз и облачный 360 Cloud для актуальной защиты в любой момент времени. На 2015 год, по стандартным настройкам антивируса, был поумолчанию активен лишь стандартный QVM движок, который сам по себе не составляет серьёзной защиты (согласно рейтингам тестирований), сторонние же движки необходимо активировать в опциях вручную. Сама по-себе эта ситуация породила рейтинговый скандал[2]. На деле же, для достижения пользователем высокой работоспособности, просто необходимо при первом запуске приложения после установки, активировать сторонние движки в опциях антивируса[3].

360 Internet Security использует проактивные технологии, чтобы предупредить, когда подозрительная программа пытается получить доступ к важным ресурсам системы, таким как настройки системы Windows, реестр, автозапуск программ и системные каталоги. Обеспечивает безопасный просмотр вебсайтов в Интернете, защиту конфиденциальности и от фишинговых сайтов, блокирует загрузку вредоносных файлов и останавливает кейлоггеры и программы для доступа к веб-камере.

Пользователи данного продукта отмечают довольно высокий уровень ложных срабатываний у встроенного движка QVM II, но при этом во многих тестах, благодаря использованию двух известных движков Avira AntiVir и Bitdefender данный антивирус показывает очень высокий уровень защиты, характерный для лучших платных антивирусов, тогда как 360 Total Security является бесплатным продуктом для персонального применения.

Версия 360 Total Security Essential отличается от основной версии отсутствием дополнительных некритичных функций для безопасности, таких как очистка реестра, кеш записей и т.п., оставляя антивирусные движки, песочницу, защиту от фишинга, троянских программ и кражи данных[4].

83.2. Системные требования

Минимальные системные требования:

Windows XP 32-bit, Vista 32-bit, Windows 7, Windows 8 и Windows 8.1 (32- и 64-bit).

Оперативная память: 512 MB Процессор: 1.6 ГГц Свободное дисковое пространство: 600 MB

83.3. Примечания

[1] Бесплатный антивирус для андроид.

[2] AV-Comparatives, AV-TEST и Virus Bulletin аннулируют сертификаты Qihoo 360 за 2015 год - Обзоры Comss.Антивирус. www.comss.ru. Проверено 15 сентября 2015.

[3] 360 Total Security Essential 7.2.0.1019 скачать бесплатно - Бесплатные антивирусы, антивирусные программы - Comss. www.comss.ru. Проверено 15 сентября 2015.

[4] 360 Total Security Essential: многоуровневая защита, защита в реальном времени и оперативное обновление. 360 Total Security. Проверено 15 сентября 2015.

83.4. Ссылки

- Русскоязычный официальный сайт антивируса
- Официальный сайт антивируса Qihoo 360

Глава 84

Rising Antivirus

84.1. О компании

“Beijing Rising International Software Co” основана в апреле 1998 года. Создана на основе компьютерного отдела разработки Beijing Rising Computer Technology (предприятие основано в 1991 г., в г. Пекине, Китай).

Компания имеет филиалы и отделения в Шанхае, Гуанчжоу, Австралии и Пекине. Является одним из крупнейших в Китае производителей антивирусного программного обеспечения, насчитывает более 500 сотрудников. (До 2010 года включительно продукт имел торговое название ЖУЙСИН и размер около 280 мБ).

84.2. Программные продукты

- Rising Antivirus
- Rising Antivirus Free Edition (бесплатен для персонального использования)
- Rising Firewall
- Rising Internet Security
- Rising PC Doctor (бесплатная утилита)

Глава 85

SafenSoft SysWatch

SafenSoft SysWatch (ранее известный как *Safe'n'Sec*[1]) — продукт для проактивной защиты от вредоносного программного обеспечения, разработанный российской компанией SafenSoft.

85.1. Редакции продукта

SafenSoft SysWatch выпускается в различных редакциях — как для персональных, так и для корпоративных пользователей.

Для домашних пользователей выпускаются следующие продукты:

- SafenSoft SysWatch Personal

Базовый продукт для обеспечения проактивной защиты компьютера от вредоносного программного обеспечения, в том числе и 0-day угроз, посредством поведенческого анализа на базе HIPS, анализируя и контролируя деятельность программ и приложений[2].

- SafenSoft SysWatch DeLuxe

Данный продукт является расширенной версией SafenSoft SysWatch Personal, обладающей, помимо проактивного компонента, функционалом классического антивирусного сканера для обнаружения и лечения вредоносных программ

85.2. Примечания

[1] *Константин Ходаковский.* SafenSoft: новые решения для надёжной защиты ПК (рус.). 3DNews (18 апреля 2011). — «Обновлённые программные решения Safe'n'Sec Personal и Safe'n'Sec Deluxe получили улучшенную функциональность и были переименованы соответственно в SysWatch Personal и SysWatch Deluxe.» Проверено 9 мая 2011. Архивировано из первоисточника 9 мая 2011.

[2] *Александр Панасенко.* Обзор SafenSoft SysWatch Deluxe (рус.). Antimalware.ru (29 апреля 2011). Проверено 9 мая 2011. Архивировано из первоисточника 9 мая 2011.

85.3. Ссылки

Официальные сайты

- SafenSoft (рус.). SafenSoft. — Официальный сайт компании. Проверено 9 мая 2011. Архивировано из первоисточника 14 мая 2012.
- Форум SafenSoft (рус.). SafenSoft. — Официальный форум компании. Проверено 2012-22-03. Архивировано из первоисточника 14 мая 2012.

Форум поддерживаемый представителями и специалистами компании http://safezone.cc/forums/forum-podderzhki-kompanii-safensoft.80/

Обзоры в прессе

- *Александр Панасенко.* Обзор SafenSoft SysWatch Deluxe (рус.). Antimalware.ru (29 апреля 2011). Проверено 9 мая 2011. Архивировано из первоисточника 9 мая 2011.

Глава 86

TrustPort a.s.

TrustPort a.s. — разработчик программного обеспечения в области информационной безопасности со штаб-квартирой в Брно, Чешская Республика. Продукция компании ориентирована на три основных направления компьютерной безопасности и защиты данных. Первым направлением является защита от вирусов, шпионских программ и вредоносных программ в общем. TrustPort реализует собственные антивирусные технологии, с использованием нескольких антивирусных ядер, лицензированных у других производителей. Второе направление — фильтрация нежелательных данных, таких как почтовый спам или веб-сайты с нежелательным содержанием. TrustPort разрабатывает технологии фильтрации, основанные на простых правилах и эвристическом анализе. Третье направление — конфиденциальность и аутентичность данных. В технологии шифрования данных и цифровой подписи используются и симметричные, и асимметричные криптосистемы. Решения от TrustPort предназначены для защиты как отдельных компьютеров, так и для защиты целых сетей.

86.1. История компании

86.1.1. До основания компании

Предшественницей TrustPort была компания AEC (изначально аббревиатура от Association for Electronics and Computers), основанная в 1991 году. Деятельность AEC распространялась на продажу программного обеспечения и предоставление услуг в сфере защиты данных. Уже в 1993 году компания приступила к разработке собственного программного обеспечения, в дополнение к продукции других производителей. Решения от AEC в 1990-е распространялись под брендом *IronWare*. Они включали, например, *IronWall* для шифрования файлов, IronBridge для защиты сетей связи, IronMail для шифрования электронной почты, и IronFolder для автоматического шифрования и дешифрования в указанных папках. Эти ранние продукты определили будущие направления для бренда TrustPort.

Позже программное обеспечение от AEC оформилось в конечном продукте *IronWare Security Suite*. В сентябре 2000 по соглашению между AEC и Norman ASA, права на *IronWare Security Suite*, а также команда разработчиков перешли к Norman ASA[1], и продукт был переименован в *Norman Security Suite*. AEC продолжала продажу программного обеспечения как бизнес-партнер Norman ASA. В марте 2002 AEC вновь начала продвижение ПО собственной разработки, представив *DataShredder*, *TrustMail* и *TrustPort Encryption* на выставке CeBIT. DataShredder был разработан для необратимого удаления конфиденциальных данных, *TrustMail* — для шифрования и подписи данных, *TrustPort Encryption* — для шифрования файлов, которое могло использоваться как на персональных компьютерах, так и на мобильных устройствах[2].

В январе 2003 года AEC запустил центр сертификации TrustPort, первый центр сертификации в Чехии, поддерживавший технологию цифровой метки времени[3]. В апреле 2003 года была выпущена вторая версия *TrustMail*, внедрившая технологию меток времени. В 2003 году началась разработка комплексного решения *TrustPort Phoenix Rebel Management*. Идея заключалась в создании единого программного решения, интегрирующего различные элементы, необходимые для компьютерной безопасности: антивирус, антиспам, межсетевой экран и шифрование. Решение предназначалось для персональных компьютеров и серверов.

К 2005 году была завершена разработка всех компонентов *TrustPort Phoenix Rebel Management*. Решение изначально было разделено на три главных продукта: *TrustPort Phoenix Rebel Workstation*; *TrustPort Phoenix Rebel Servers*, в составе которого шли антивирус-шлюз, антиспам-шлюз и сетевой брандмауэр; и *TrustPort Phoenix Rebel Management*. Позднее первый продукт стал известен как *TrustPort Workstation*, второй — *TrustPort Gateway*. В мае 2007 года AEC представила *TrustPort WebFilter*, продукт для блокирования нежелательного веб-контента.

86.1.2. После основания компании

В ноябре 2007 года было подписано соглашение о приобретении AEC компанией Cleverlance. Cleverlance как новый владелец AEC принял стратегическое решение о создании автономной компании из отдела разработок AEC. В марте 2008 года, новая компания была официально внесена в торговый реестр Чешской Республики, под названием TrustPort. Главой стал Йежи Мрнуштик (Jiří Mrnuštík)[4]. AEC продолжила продажу продуктов TrustPort в статусе реселлера TrustPort. После выхода TrustPort из состава AEC обе компании — AEC и TrustPort — переехали в новый офис в офисном центре Spielberk в июне 2008 года.

В апреле 2008 года произошли два важных изменения в продуктовой линейке TrustPort. *Workstation* был переименован в *TrustPort PC Security*, как альтернатива решениям той же категории от конкурирующих разработчиков[5]. В то же время, *TrustPort Antivirus* был внедрен в качестве обособленного продукта для пользователей, не нуждающихся в полном пакете решений, а лишь в решении, достаточном для защиты от вредоносного ПО. В ноябре 2008 года на рынок была представлена обновленная линия продуктов, состоящая из *TrustPort Antivirus 2009* и *TrustPort PC Security 2009*[6][7]. Был обновлен графический интерфейс пользователя, внедрена технология родительского контроля и ряд других функций. Январь 2009 года ознаменовал запуск *TrustPort Antivirus USB Edition*, который вскоре был переименован в *TrustPort USB Antivirus*, часть антивирусного программного обеспечения, разработанного специально для защиты флэш-накопителей[8][9].

В феврале 2009 года произошли изменения в руководстве компании. Владислав Немец (Vladislav Němec) был назначен новым главным исполнительным директором TrustPort. На протяжении всего года, были подписаны и усилены соглашения о деловом партнерстве с несколькими важными дистрибьюторами по всему миру: в Великобритании, Канаде, Италии, Индии, Мексике, Испании и Франции. В ноябре 2009 года *TrustPort Antivirus 2010* и *TrustPort PC Security 2010* были выпущены для продажи[10]. В число нововведений были включены функция автоматизированного обновления, расширения для почтовых клиентов и опция выбора языка в любое время. В апреле 2010 года *TrustPort Esign Pro Extended* дополнила текущий портфель продуктов[11].

В декабре 2009 года на русский язык было переведено офисом в Казахстане[12] основное решение для защиты информации — TrustPort Antivirus 2010. Это и стало новым шагом для популяризации решения в СНГ. Возглавил этот процесс директор представительства, Станислав Кусков (Stanislav Kuskov).

В целях удовлетворения потребностей различных сегментов пользователей, компания изменила продуктовый портфель в сентябре 2010 года[13]. Для домашних пользователей и малых офисов, были введены три альтернативных продукта вместо прежних двух: *TrustPort Antivirus 2011*, *TrustPort Internet Security 2011* и *TrustPort Total Protection 2011*. Для среднего и крупного бизнеса было представлено комплексное решение TrustPort Security Elements с четырьмя различными уровнями защиты. TrustPort Security Elements был разработан как комплект программного обеспечения, который будет защищать различные элементы гетерогенной сети.

В первой половине 2011 года был полностью переведён на русский язык интерфейс продуктов линейки @Home (*Antivirus, Internet Security, Total Protection*) и *TrustPort Antivirus for Server*. Перевод выполнил российский дистрибутор TrustPort — компания Дина-Софт.

13 июля 2011 года была выпущена обновлённая линейка продуктов 2012. Одним из самых важных новшеств является *Application Inspector* (Инспектор приложений), позволяющий блокировать вредоносные или подозрительные действия программ в системных областях ОС.

13 октября 2011 года TrustPort представил новый продукт для защиты конфиденциальных данных — TrustPort Tools 2012. Решение идеально подходит для предприятий и частных лиц, которые хотят дополнить свои антивирусные решения средствами защиты данных. TrustPort Tools 2012 содержит модули для оффлайн и онлайн шифрования данных, а также дает возможность безвозвратного удаления конфиденциальных данных без возможности их восстановления.

86.2. Продукция

86.2.1. TrustPort @home

TrustPort Antivirus — это базовое решение для пользователей ПК для защиты от вирусов, шпионских программ и любого другого вредоносного ПО. Представлен в трех следующих вариантах.

TrustPort Antivirus: сканирование по требованию, сканирование по доступу, постоянная антивирусная защита, превентивный контроль, автоматический контроль съемных носителей, инспектор приложений, автоматическое и ручное обновление.

TrustPort Internet Security — добавлен антиспам и антишпион, веб-сканирование, персональный файервол, возможность родительского контроля и создания мобильного антивируса на съемных носителях.

TrustPort Total Protection — наиболее совершенный по функциональности вариант, включающий также возможность шифрования виртуальных дис-

ков, архивов, шреддинг, создание загрузочного диска восстановления системы, управление доступом к каталогам.

Поддерживаются платформы Windows 7, Windows Vista, Windows XP, Windows 2000. В настоящее время доступны мультиязычные версии продуктов. Язык интерфейса (английский, русский, чешский, итальянский, немецкий, португальский, испанский, польский, венгерский) можно выбрать в процессе установки продукта или поменять позже.

86.2.2. TrustPort @office

TrustPort Security Elements — корпоративное решение для централизованного управления защитой компьютеров сети, веб-фильтрации, защиты файловых серверов, шифрования и безопасного уничтожения данных. Имеет 4 уровня защиты.

TrustPort eSign Pro — программа для безопасного обмена документами, при котором реципиент получает гарантию происхождения, неприкосновенности и сохранности документа. Включает технологии электронной подписи, шифрования данных и меток времени. Также поддерживает документы формата PDF.

TrustPort Small Business Server — решение для защиты серверов от вредоносного ПО.

TrustPort USB Antivirus — решение для защиты съемных носителей путем установки мобильного антивируса.

86.2.3. TrustPort @enterprise

TrustPort Net Gateway обеспечивает защиту периметра корпоративной сети от вредоносного ПО и спама. TrustPort Net Gateway содержит антивирус, многоуровневый антиспам, антишпион, веб-фильтр, и обеспечивает безопасность периметра корпоративной сети.

TrustPort WebFilter блокирует посещение сетевыми пользователями нежелательных и опасных вебсайтов, несанкционированную загрузку файлов. В состав TrustPort WebFilter входит веб-фильтрация, за счет чего обеспечивается оптимизация интернет-соединений.

86.2.4. Другие решения

TrustPort Tools 2012 содержит модули для шифрования данных, а также предоставляет возможность безвозвратного удаления конфиденциальных данных без возможности их восстановления.

TrustPort Certification Authority — серверное программное обеспечение для выпуска, проверки и аннулирования цифровых сертификатов.

TrustPort Timestamp Authority — серверное программное обеспечение для выпуска меток времени, подтверждающих существование документа в определенный момент времени.

TrustPort PKI SDK — набор инструментов для создания и изменения приложений посредством изначальной инфраструктуры открытых ключей (PKI).

86.3. Независимые тесты

Решения от TrustPort регулярно проходят тестирование независимых лабораторий и получают награды. В октябре 2006 года *TrustPort Antivirus* прошел тест Virus Bulletin, по результатам которого в первый раз получил награду *VB100*. В том же месяце по результатам теста *AV-Comparatives* была получена первая награда *AV-Comparatives Advanced+*[14]. В феврале 2009 *TrustPort PC Security* тестировался *PC Security Labs* и впервые получил *PC Security Labs Excellent*. В январе 2010, *West Coast Labs* тестировал *TrustPort Antivirus*. По результатам продукт получил награду *Checkmark* в двух категориях[15].

В 2011 году *TrustPort Antivirus* участвовал в тестировании Virus Bulletin три раза. Тестирование проводилось на платформах Windows XP Professional (апрель), Windows Server 2008 R2 (июнь) и Windows Vista SP2 x64 Business (август). На всех платформах *TrustPort Antivirus* показал наилучший уровень детектирования без ложных срабатываний.

86.4. Примечания

[1] Norman acquires PKI technology and competence

[2] AEC na Cebitu 2002

[3] E-podpis aneb testujeme digitální certifikáty

[4] TrustPort Inc. initiated its operation in full extent

[5] TrustPort Workstation is changing its name to TrustPort PC Security

[6] TrustPort PC Security 2009 official release

[7] TrustPort PC Security 2009: brněnský přístav bezpečí

[8] TrustPort unveils two portable antivirus products

[9] Portable antivirus software to keep your data safe

[10] TrustPort rolls out new versions of its antivirus solutions

[11] TrustPort eSign Pro extends TrustPort product portfolio

[12] TrustPort | Казахстан — антивирус, антишпион, антиспам, файрволл — защита информации, защита сетей

[13] TrustPort is fundamentally changing its product portfolio

[14] TrustPort Antivirus uspěl v testech na spyware a další nechtěný software

[15] West Coast Labs Checkmark illustrates the quality of TrustPort products

86.5. Ссылки

- Официальный сайт
- Русская версия сайта

Глава 87

TrustPort Antivirus

TrustPort Antivirus — антивирусный пакет, выпускаемый чешским разработчиком программного обеспечения в области информационной безопасности TrustPort a.s.. Является мультисканерным антивирусным решением.

87.1. История

В 1990-е годы материнская компания AEC разрабатывала решения для защиты данных под брендом IronWare. В 2000 году права на IronWare Security Suite перешли во владение норвежской Norman ASA [1], а AEC начал новый проект, и в 2002 году на выставке CeBIT представила DataShredder, TrustMail и TrustPort Encryption. В январе 2003 года AEC запустил центр сертификации TrustPort, первый центр сертификации в Чехии, поддерживавший технологию цифровой метки времени. Также в 2003 году началась разработка комплексного решения TrustPort Phoenix Rebel Management, которая была окончена в 2005 году.

В 2007 году после приобретения AEC компанией Cleverlance [2] была создана независимая дочерняя компания TrustPort A.S. В ноябре 2008 года на рынок была представлена обновленная линия продуктов, состоящая из TrustPort Antivirus 2009 и TrustPort PC Security 2009. Январь 2009 года ознаменовал запуск TrustPort Antivirus USB Edition.

Для популяризации базового решения для защиты компьютера от вирусов (TrustPort Antivirus 2010), в декабре 2009 года оно было переведено на русский язык. Перевод был осуществлен казахстанским офисом.

В апреле 2010 года TrustPort eSign Pro Extended дополнила текущий портфель продуктов.

В сентябре 2010 года для домашних пользователей и малых офисов были введены три альтернативных продукта: TrustPort Antivirus 2011, TrustPort Internet Security 2011 и TrustPort Total Protection 2011. Для среднего и крупного бизнеса было представлено комплексное решение TrustPort Security Elements.

В первой половине 2011 года был полностью переведён на русский язык интерфейс ряда продуктов TrustPort (Antivirus, Internet Security, Total Protection). Перевод выполнил российский дистрибутор TrustPort - компания ДинаСофт.

13 июля 2011 года была выпущена обновлённая линейка продуктов 2012. Одним из самых важных новшеств является Application Inspector (Инспектор приложений), позволяющий блокировать вредоносные или подозрительные действия программ в системных областях ОС.

87.2. TrustPort @home

TrustPort предлагает пользователям линейку продуктов для защиты от вирусов, шпионских программ и любого другого вредоносного ПО. В домашних продуктах TrustPort используется два высокотехнологичных сканера(движка). Доступны следующие варианты:

TrustPort Antivirus 2013: сканирование по требованию, сканирование по доступу, постоянный антивирусный щит, превентивный контроль, автоматический контроль съемных носителей, автоматическое и ручное обновление.

TrustPort Internet Security 2013 - добавлен антиспам и антишпион, веб-сканирование, персональный файервол, возможность родительского контроля и создания мобильного антивируса на съемных носителях.

TrustPort Total Protection 2013 – наиболее совершенный по функциональности вариант, включающий также возможность шифрования виртуальных дисков, архивов, создание мобильного антивируса на съемных носителях. шреддинг и восстановление загрузочного диска.

TrustPort USB Antivirus – мобильная версия антивируса с возможностью шифрования данных. (Используется один сканер).

Поддерживаются платформы Windows 7, Windows Vista, Windows XP, Windows 2000. В настоящее время доступны мультиязычные версии продуктов. Язык

интерфейса (английский, русский, чешский, итальянский, немецкий, португальский, испанский, польский, венгерский) можно выбрать в процессе установки продукта или поменять позже.

87.3. TrustPort @office

TrustPort Security Elements — корпоративное решение для централизованного управления защитой компьютеров сети, веб-фильтрации, защиты файловых серверов, шифрования и безопасного уничтожения данных. Имеет 4 уровня защиты.

TrustPort eSign Pro – программа для безопасного обмена документами, при котором реципиент получает гарантию происхождения, неприкосновенности и сохранности документа. Включает технологии электронной подписи, шифрования данных и меток времени. Также поддерживает документы формата PDF.

TrustPort Small Business Server – решение для защиты серверов от вредоносного ПО.

TrustPort USB Antivirus – решение для защиты съемных носителей путем установки мобильного антивируса.

87.4. TrustPort @enterprise

TrustPort Net Gateway обеспечивает защиту периметра корпоративной сети от вредоносного ПО и спама. TrustPort Net Gateway содержит антивирус, многоуровневый антиспам, антишпион, веб-фильтр, и обеспечивает безопасность периметра корпоративной сети.

TrustPort WebFilter блокирует посещение сетевыми пользователями нежелательных и опасных вебсайтов, несанкционированную загрузку файлов. В состав TrustPort WebFilter входит веб-фильтрация, за счет чего обеспечивается оптимизация интернетсоединений.

87.5. Примечания

[1] Norman ASA

[2] Cleverlance

87.6. Ссылки

- Официальный сайт TrustPort
- Казахстанский сайт TrustPort
- Российская версия сайта
- Украинский сайт TrustPort
- сайт TrustPort в Республике Молдова
- Альтернативный Российский сайт (НКО TrustPort Russia)

Глава 88

TrustPort Security Elements

TrustPort Security Elements — решение для комплексной защиты корпоративных сетей и отдельных их компонентов, разрабатываемое чешской компанией TrustPort a.s. Представлен в 4 версиях, различающихся степени функциональности: Basic, Advanced, Premium, Ultimate.

88.1. TrustPort Security Elements и используемые компоненты

Глава 89

USB Disk Security

USB Disk Security (также **USBGuard**) — антивирусная утилита для операционных систем Microsoft Windows. Разработка компании Zbshareware Lab, распространяется по лицензии Adware и Shareware. Предназначена для обнаружения и удаления компьютерных вирусов, пытающихся заразить компьютер через флеш-накопители, в частности защищает от потенциально опасных файлов Autorun.inf. Программа не является полноценным антивирусом, её рекомендуется использовать только как дополнение к основному антивирусу.

89.1. Возможности программы

- Резидентный антивирусный сканер, который срабатывает при подключении нового флеш-накопителя к системе. По умолчанию вирусы удаляются автоматически.
- Возможность более тщательно просканировать внешний накопитель. В случае обнаружения вирусов они либо перемещаются в карантин, либо удаляются.
- Возможность просмотреть содержимое накопителя без риска заразить компьютер.
- Возможность полностью отключить автозапуск на компьютере.
- Возможность безопасного веб-сёрфинга через поисковый сервис linkzb.com.
- Проверка сайтов на наличие вирусов. Для проверки используются сервисы VirusTotal, Google, McAfee, Symantec и Trend Micro.
- Инструмент *USB Access Control*, блокировка несанкционированного копирования данных на USB-диски.
- Инструмент *USB Drive Control*, предотвращение несанкционированного подключения USB-дисков к компьютеру.
- Наличие защиты настроек программы паролем.
- Имеется встроенная система очистки временных файлов, что также позволит удалить вирусы, если они окажутся во временных каталогах.
- Имеется встроенная система восстановления важных веток в реестре, которые были изменены вредоносными программами.
- Возможность управления программами, записанными в автозапуск.
- Программа не требует обновления сигнатурных баз вирусов, поскольку работает не как стандартный антивирус.
- Автоматическая проверка обновлений программы.
- Программа совместима практически со всеми современными антивирусами.
- Потребляет очень мало ресурсов, благодаря чему её можно установить даже на очень слабые машины.
- Многоязычный интерфейс, поддержка 13 языков.

89.2. Лицензия

Раньше программа являлась условно-бесплатной, стоимость полной лицензии составляла 55 долларов. После оплаты пользователю присылался регистрационный ключ, имеющий неограниченный срок действия. Все последующие обновления также были бесплатны. Незарегистрированная версия имела ограничение - в случае обнаружения вируса она его не удаляла.

Начиная с версии 6.3.0 у разработчиков появился спонсор, благодаря которому программа стала бесплатной.

89.3. Критика

В большинстве случаев программа получает положительные отзывы, однако иногда подвергают критике. Чаще всего из-за рекламной акции разработчиков, утверждающей, что их программа способна обеспечить 100% защиту от угроз с внешних накопителей, однако это вовсе не так. В связи с этим критике подвергалась и слишком завышенная цена программного продукта (на тот момент, когда он был платным). Имеется множество сообщений о ложных срабатываниях, в результате которых программа удаляла вполне безобидные файлы. Некоторые пользователи утверждают, что подобного рода программы не нужны и вовсе, потому как автозапуск приложений на компьютере можно отключить вручную.

89.4. Интересный факт

- Ярлык пятой версии программы очень сильно напоминал ярлык Антивируса Касперского. Начиная с шестой его заменил красно-белый щит.

89.5. Ссылки

- Официальный сайт программы (англ.). Архивировано из первоисточника 16 мая 2012.
- Официальный сайт программы (русскоязычный раздел). Архивировано из первоисточника 16 мая 2012.
- Обзор журнала Домашний ПК. Архивировано из первоисточника 16 мая 2012.
- Обзор программы (англ.). Softpedia.
- Обзор на сайте SoftSalad. Архивировано из первоисточника 16 мая 2012.

Глава 90

VirusTotal

VirusTotal — бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ. VirusTotal награждён Американским изданием PC World Magazine как один из 100 лучших продуктов 2007 года.[1]

Имел локализацию на многие языки мира, включая русский. После обновления доступен только английский вариант. При выборе языка предлагается помочь с локализацией. В феврале 2013 появилось ещё шесть языков интерфейса.[2]

90.1. Описание

Сервис является полностью бесплатным, не принуждая пользователя ни к прямым, ни к косвенным тратам.

Результаты проверок файлов сервисом не зависят от какого-то одного производителя антивирусов. В VirusTotal используется несколько десятков антивирусных систем, что может позволить делать более надёжные выводы об опасности файла, по сравнению с каким-то одним продуктом, выявлять ложные срабатывания какого-то одного антивируса, либо, наоборот, несрабатывания на свежую угрозу, возможно, уже внесённую другими производителями в свои базы.

У компаний-разработчиков антивирусного программного обеспечения существуют собственные классификации и номенклатуры вредоносных программ, поэтому при проверке файла антивирусы на Virustotal могут выдавать разные результаты, например, одни антивирусы посчитают файл опасным, а другие безопасным.

Если антивирусы на Virustotal не обнаружили угрозу, Virustotal пишет, что файл «**Похоже, безвреден!** С большой долей уверенности можно предположить, что файл безопасен для использования.», и не гарантирует 100 % отсутствие вредоносного кода в файле.

Все используемые сервисом антивирусные базы постоянно обновляются. В результатах проверки указываются даты последних обновлений всех баз.

После загрузки файла система вычисляет его хэш и при наличии результатов проверки файла с таким же хэшем сразу выдаст их пользователю, с указанием всех подробностей, включая дату проверки. При этом возможно повторить проверку на текущий момент, с текущими обновлениями баз.

На сайте можно посмотреть статистику по проведённым проверкам в реальном времени. Например, *Топ 10 заражённых файлов за последние сутки*.

Сервис постоянно развивается[3], постоянно подключаются новые сканеры (антивирусы и антитрояны).

VirusTotal отсылает подозрительные файлы производителям антивирусов на анализ.[4]

7 сентября 2012 года в блоге сайта было объявлено о приобретении сервиса компанией Google[5].

90.2. Антивирусные движки, используемые в сервисе для проверки файлов

*AegisLab (AegisLab)

- Agnitum (Agnitum)
- AhnLab (V3)
- Alibaba Group (Alibaba)
- Antiy Labs (Antiy-AVL)
- ALWIL (Avast! Antivirus)
- Arcabit (Arcabit)
- AVG Technologies (AVG)
- Avira (AntiVir)
- BluePex (AVware)
- Baidu (Baidu-International)
- BitDefender GmbH (BitDefender)

- Bkav Corporation (Bkav)
- ByteHero Information Security Technology Team (ByteHero)
- Cat Computer Services (Quick Heal)
- CMC InfoSec (CMC Antivirus)
- Cyren (Cyren)
- ClamAV (ClamAV)
- Comodo (Comodo)
- Doctor Web, Ltd. (DrWeb)
- ESTsoft (ALYac)
- Emsi Software GmbH (Emsisoft)
- Eset Software (ESET NOD32)
- Fortinet (Fortinet)
- FRISK Software (F-Prot)
- F-Secure (F-Secure)
- G DATA Software (GData)
- Hacksoft (The Hacker)
- Hauri (ViRobot)
- Ikarus Software (Ikarus)
- INCA Internet (nProtect)
- Jiangmin
- K7 Computing (K7AntiVirus, K7GW)
- Kaspersky Lab (Kaspersky)
- Kingsoft (Kingsoft)
- Lavasoft (Ad-Aware)
- Malwarebytes Corporation (Malwarebytes Anti-malware)
- Intel Security (McAfee)
- Microsoft (Malware Protection)
- Microworld (eScan)
- Nano Security (Nano Antivirus)
- Panda Security (Panda Platinum)
- Qihoo 360 (Qihoo 360)
- Rising Antivirus (Rising)
- Sophos (SAV)
- SUPERAntiSpyware (SUPERAntiSpyware)
- Symantec Corporation (Symantec)
- Tencent (Tencent)
- ThreatTrack Security (VIPRE Antivirus)
- TotalDefense (TotalDefense)
- Trend Micro (TrendMicro, TrendMicro-HouseCall)
- VirusBlokAda (VBA32)
- Zillya! (Zillya)
- Zoner Software (Zoner Antivirus)

90.3. Антивирусные движки, используемые в сервисе для проверки URL-адреса

- ADMINUSLabs (ADMINUSLABS)
- AegisLab WebGuard (AegisLab)
- Alexa (Amazon)
- AlienVault (AlienVault)
- Antiy-AVL (Antiy Labs)
- AutoShun (RiskAnalytics)
- Avira Checkurl (Avira)
- Baidu-International (Baidu)
- BitDefender (BitDefender)
- Blueliv (Blueliv)
- CRDF (CRDF FRANCE)
- C-SIRT (Cyscon SIRT)
- CLEAN MX (CLEAN MX)
- Comodo Site Inspector (Comodo Group)
- CyberCrime (Xylitol)
- Dr.Web Link Scanner (Dr.Web)
- Emsisoft (Emsi Software GmbH)
- ESET (ESET)
- FortiGuard Web Filtering (Fortinet)
- FraudSense (FraudSense)
- G-Data (G Data)
- Google Safebrowsing (Google)
- K7AntiVirus (K7 Computing)

- Kaspersky URL advisor (Kaspersky)
- Malc0de Database (Malc0de)
- Malekal (Malekal's MalwareDB)
- Malwarebytes hpHosts (Malwarebytes)
- Malwared (Malware Must Die)
- Malware Domain Blocklist (DNS-BH - Malware Domain Blocklist)
- Malware Domain List (Malware Domain List)
- MalwarePatrol (MalwarePatrol)
- Malwares.com (Saint Security)
- Netcraft (Netcraft)
- OpenPhish (FraudSense)
- Opera (Opera)
- Palevo Tracker (Abuse.ch)
- ParetoLogic URL Clearing House (ParetoLogic) more info
- Phishtank (OpenDNS)
- Quttera (Quttera)
- Rising (Rising)
- SCUMWARE (Scumware.org)
- SecureBrain (SecureBrain)
- Sophos (Sophos)
- Spam404 (Spam404)
- SpyEye Tracker (Abuse.ch)
- StopBadware (StopBadware)
- Sucuri SiteCheck (Sucuri)
- ThreatHive (The Malwarelab)
- Trend Micro Site Safety Center (Trend Micro)
- Trustwave (Trustwave)
- urlQuery (urlQuery.net)
- VX Vault (VX Vault)
- Web Security Guard (Crawler, LLC)
- Websense ThreatSeeker (Websense)
- Webutation (Webutation)
- Wepawet (iseclab.org)
- Yandex Safebrowsing (Yandex)
- ZCloudsec (Zcloudsec)
- ZDB Zeus (ZDB Zeus)
- Zeus Tracker (Abuse.ch)
- Zvelo (Zvelo)

90.4. Ограничения сервиса

Несмотря на все достоинства онлайновой проверки, сервис ни в коем случае не заменяет антивирус на локальном компьютере, поскольку проверяются только отдельные файлы по требованию и отдельные URL-адреса. Сервис не обеспечивает постоянную защиту на компьютере пользователя и является дополнением к установленному антивирусу. Хотя сервис и использует несколько антивирусных движков, результат антивирусов не гарантирует безвредность файла или URL-ссылки. Более того, совокупный объем ложных срабатываний на сервисе у нескольких антивирусов выше, чем у отдельного сканера или антивируса. В настоящее время не существует ни одного антивируса, который давал бы 100% эффективность обнаружения вредоносных программ и вредоносных URL-адресов Об этом прямо заявляют авторы проекта[6]. Максимальный размер загружаемого файла ограничен 128 мегабайтами.

Virustotal не предназначен для сравнения антивирусов по следующим причинам (об этом прямо заявляют авторы проекта) - антивирусные движки на Virustotal работают по-другому, не так, как антивирусы в настольных компьютерах. Например, эвристический анализ в антивирусных движках на Virustotal может быть более "агрессивным" и параноидальным, чем в антивирусах, установленных на компьютере пользователя с настройками по умолчанию.

Согласно санкционной политике США против жителей Республики Крым, сервис не доступен жителям Республики Крым, как и многие другие сервисы компании Google.

90.5. Недостатки сервиса

- Статистика на сайте показывается «как есть», нет ни средств, ни возможностей для её анализа.
- API имеет ограничение по лимиту запросов и по размеру файла, как в бесплатной версии, так и в корпоративной (платной) версии.

90.6. Примечания

[1] The 100 Best Products of 2007 - PC World (англ.). Архивировано из первоисточника 23 марта 2012.

[2] сообщение в твиттере (англ.)

[3] История развития сервиса VirusTotal

[4] https://www.virustotal.com/faq «as a tool that checks suspicious samples with several antivirus solutions and helps antivirus labs by forwarding them the malware they fail to detect.»

[5] An update from VirusTotal (7 сентября 2012). Проверено 8 сентября 2012. Архивировано из первоисточника 19 октября 2012. (англ.)

[6] О VirusTotal

90.7. Ссылки

- virustotal.com/
- Антивирусы онлайн — обзор онлайн-антивирусов

Глава 91

Windows Live OneCare

Windows Live OneCare (до этого известный как **Windows OneCare Live** и имеющий кодовое название **A1**) — антивирусная программа от Microsoft.

В 2009 Microsoft закрыла проект.

91.1. История

До выпуска первой известной версии OneCare носил кодовое имя A1. Windows Live OneCare вступила в бета-стадию летом 2005 года. Затем началось публичное бета-тестирование. 31 мая 2006 года первая версия Windows Live OneCare появилась в розничных магазинах в США.

В начале октября 2006 года Microsoft выпустила бета-версию Windows Live OneCare 1.5. Версия 1.5 была выпущена 3 января 2007 года и была представлена общественности 30 января 2007 года.

4 июля 2007 года, началось бета-тестирование версии 2.0, а окончательный вариант был выпущен 16 ноября 2007 года.

Windows Live OneCare 2.5 (2.5.2900.3) окончательно был выпущен 3 июля 2008 года. В тот же день Microsoft выпустила серверную версию Windows Live OneCare 2.5.

Поддержка Windows Live OneCare прекращена 30 июня 2009 года.

91.2. Функции

Windows Live OneCare включает в себ интегрированный антивирус, межсетевой экран, утилиты для создания резервных копий и восстановления, утилиту для настройки системы, а также возможность интеграции с Windows Defender для защиты от malware.

91.2.1. Совместимость

OneCare версии 1.5 совместим только с 32 битными версиями Windows XP и Windows Vista[1]. OneCare версии 2 поддерживает 64 битную версию Vista.

91.2.2. Активация

Windows Live OneCare требует пользователя активировать продукт, если он захочет использовать его после пробного периода (90 дней). Активация может быть произведена при наличии действующей учетной записи Windows Live ID, поэтому может быть проведена ассоциация подписки на OneCare и учетной записи. Когда продукт активирован, серая панель наверху программы пропадает и подписка полностью активируется на один год, начиная с даты активации. Пользователи могут проверить статус их подписки на странице биллинга.

Windows Live OneCare не требует проверки подлинности Windows с помощью Windows Genuine Advantage.

91.3. См. также

- Microsoft Security Essentials

91.4. Примечания

[1] Microsoft Watch — Security — Next Release of OneCare Won't Support Vista x64

Глава 92

Zillya!

Zillya! Антивирус — бесплатный антивирус от украинской антивирусной лаборатории «Лаборатория Zillya!», первая версия которого появилась в апреле 2009 года. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, рекламных программ, а также неизвестных угроз с помощью проактивной защиты.

92.1. Функции

92.1.1. Основные возможности

- Защита от вирусов, червей, троянов и других вредоносных программ.
- Защита от шпионских и рекламных программ.
- Защита от несанкционированного доступа к личной информации.
- Функция слежения в режиме реального времени («Сторожевой»).
- Встроенный алгоритм эвристического анализа.
- Проверка файлов загружаемых на компьютер из сети Интернет.
- Почтовый фильтр.
- Проверка офисных документов.

92.1.2. Дополнительные возможности

- Диспетчер задач и Диспетчер автозагрузки, расширяют функциональность программы и помогают пользователю лучше контролировать процессы в системе.
- Встроенная функция отправки файлов на анализ в лабораторию.
- Выбор режимов сканирования и сканирование по расписанию.

92.1.3. Удобство

- Информативные диалоговые окна для принятия пользователем обоснованных решений.
- Возможность выбора между автоматическим и интерактивным режимами работы.
- Автоматическое обновление баз и программы.
- Украиноязычная и русскоязычная техподдержка.

92.1.4. Системные требования

Частота процессора: 1 ГГц или выше.

Оперативная память: 512 Мб или более.

Место на жестком диске: 120 Мб.

Операционная система: Windows XP (SP2, SP3), Windows Vista, Windows 7 (32-х и 64-х битные), Windows 8 (x32, x64).

92.2. Ссылки

- Официальный сайт
- Zillya! — первый бесплатный украинский антивирус
- Обзор Zillya! Антивирус

Глава 93

Антивирус Касперского

Антиви́рус Каспе́рского (англ. *Kaspersky Antivirus, KAV*) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS (только для старших версий, именуемых «Kaspersky Internet Security 2009+, где '+' — порядковый номер предыдущего регистра, ежегодно увеличиваемый на единицу в соответствии с номером года, следующим за годом выпуска очередной версии антивируса»). Первоначально, в начале 1990-х, именовался **-V**, затем — **AntiViral Toolkit Pro**.

Кроме собственно антивируса, также выпускается бесплатная лечащая утилита Kaspersky Virus Removal Tool.

93.1. Функции

93.1.1. Базовая защита

- Защита от вирусов, троянских программ и червей
- Защита от шпионских и рекламных программ
- Проверка файлов в автоматическом режиме и по требованию
- Проверка почтовых сообщений (для любых почтовых клиентов)
- Проверка интернет-трафика (для любых интернет-браузеров)
- Защита интернет-пейджеров (ICQ, MSN)
- Мониторинг активности (собирает данные о действиях программ на компьютере и предоставляет эту информацию другим компонентам для более эффективной защиты).
- **Защита от программ-эксплойтов.**
- **Защита от программ блокировки экрана.**
- **Откат действий вредоносной программы (**позволяет выполнить отмену всех совершенных программой действий, если программа будет признана вредоносной**).**
- **Защита от троянов-шифровальщиков**
- Проверка Java- и Visual Basic-скриптов
- Защита от скрытых битых ссылок
- Постоянная проверка файлов в автономном режиме
- Постоянная защита от фишинговых сайтов

93.1.2. Предотвращение угроз

- Поиск уязвимостей в ОС и установленном ПО
- Анализ и устранение уязвимостей в браузере Internet Explorer
- Блокирование ссылок на заражённые сайты
- Распознавание вирусов по способу их упаковки
- Глобальный мониторинг угроз (Kaspersky Security Network)

93.1.3. Восстановление системы и данных

- Возможность установки программы на заражённый компьютер
- Функция самозащиты программы от выключения или остановки
- Восстановление корректных настроек системы после удаления вредоносного ПО
- Наличие инструментов для создания диска аварийного восстановления

93.1.4. Защита конфиденциальных данных

- Блокирование ссылок на фишинговые сайты
- Защита от всех видов кейлоггеров

93.1.5. Удобство использования

- Автоматическая настройка программы в процессе установки
- Готовые решения (для типичных проблем)
- Наглядное отображение результатов работы программы
- Информативные диалоговые окна для принятия пользователем обоснованных решений
- Возможность выбора между простым (автоматическим) и интерактивным режимами работы
- Круглосуточная техническая поддержка
- Автоматическое обновление баз

93.2. Системные требования

93.2.1. Общие требования для всех операционных систем

- Около 480 Мб свободного пространства на жёстком диске (в зависимости от размера антивирусных баз)
- CD-ROM для установки программы с диска
- Компьютерная мышь
- Подключение к интернету для активации продукта и получения регулярных обновлений
- Microsoft Internet Explorer 6.0 или выше
- Microsoft Windows Installer 2.0 или выше

93.2.2. Аппаратные требования для нетбуков

- Процессор: Intel Atom 1.6 ГГц
- Видеокарта: Intel GMA950
- Экран: 10.1”
- Операционная система: Microsoft Windows XP Home Edition

93.3. Статус поддержки программы

93.4. Награды

- По состоянию на январь 2010 года Антивирус Касперского имеет 51 награду VB100 от Virus Bulletin.[2][3]
- Антивирус имеет следующие награды российского портала AntiMalware: Gold Packers Support (август 2006)[4], Silver Malware Treatment Award Gold (сентябрь 2007)[5], Anti-Rootkit Protection Award (декабрь 2007)[6], Silver Proactive Protection Award (декабрь 2007)[7], Gold Anti-Polymorphic Protection Award (февраль 2008)[8], Silver Performance Award: System Startup, Silver Performance Award On-Access Scanning, Bronze Performance Award On-Demand Scanning, Bronze Performance Award Office Software (август 2008)[9], Gold Malware Treatment Award (октябрь 2008)[9], Gold Self-Protection Award (август 2007 и январь 2009)[10][11], Gold Proactive Protection Award (март 2009)[12], Gold Zero-day Protection Award (ноябрь 2009)[13].
- Март 2009 года — Антивирус Касперского 2009 удостоен отраслевой премии Choice of Channel 2008 в категории «Лучшая новинка года». Победителей профессионального конкурса Choice of Channel 2008 определяли компании-лидеры компьютерной индустрии, представители крупнейших розничных сетей, а также магазинов компьютерной техники и ПО в странах Ближнего Востока.
- Май 2009 года — Антивирус Касперского 2009 снова получил максимальную оценку тестовой лаборатории AV-Comparatives[14].

93.5. Критика

Антивирус часто получает положительные отзывы за достаточно высокий уровень выявления вредоносных программ, как и часто критикуется пользователями, за большое количество ложных срабатываний. По данным независимых исследований, Касперский является одним из самых продаваемых антивирусов в России[15]. Однако у Антивируса Касперского отмечаются и недостатки. Один из самых известных, — крайне большая ресурсоёмкость программы. На слабых и средних компьютерах это может заметно мешать работе пользователя, а в некоторых случаях приводить к стопроцентной нагрузке процессора и, как следствие, зависанию компьютера (особен-

но во время обновления вирусных баз). Сам Евгений Касперский утверждает, что замедление работы уже давно в прошлом[16], это подтверждают последние тесты антивирусов[17]. Также в Интернете можно найти немало обзоров, в которых опровергается миф, что Антивирус Касперского тормозит[18], но часто такие обзоры подвергаются критике со стороны пользователей[*каких?*].

Антивирус Касперского критикуют за его избыточную назойливость. Например, он добавлял свою эмблему на экран приветствия, что многими пользователями расценивается, как попытка лишний раз обратить на себя внимания (убрано в последних версиях), как и знаменитый «поросячий визг» — звук при обнаружении вирусов в старых версиях программы, который пугал большинство пользователей. И хотя этот звук убрали в седьмой версии программы, у многих пользователей антивирус Касперского ассоциируется с этим звуком.

93.6. «Пасхальное яйцо»

Если в титрах, идущих в окне «О программе» версий, начиная с версии 7.0[19] щёлкнуть мышью по имени Евгения Касперского, появляется фото, где он показывает «Превед!». Стойка Евгения Касперского в точности повторяет стойку медведя из русской редакции картины «Bear Surprise» Джона Лури.

93.7. См. также

- Kaspersky Internet Security
- Kaspersky CRYSTAL
- Kaspersky Password Manager
- Kaspersky Mobile Security

93.8. Примечания

[1] Статус поддержки программ для защиты персональных компьютеров. Официальный сайт технической поддержки. Проверено 4 сентября 2012. Архивировано из первоисточника 18 октября 2012.

[2] Virus Bulletin : VB100 results — Kaspersky

[3] Virus Bulletin : VB100 results — Kaspersky AntiVirus 2010

[4] Результаты теста антивирусов на поддержку упаковщиков — Тесты и сравнения антивирусов — Anti-Malware.ru

[5] Результаты теста антивирусов на лечение активного заражения (сентябрь 2007) — Тесты и сравнения антивирусов — Anti-Malware.ru

[6] Результаты теста антивирусов и антируткитов на обнаружение и удаление современных руткитов (декабрь 2007) — Тесты и сравнения антивирусов — Anti-Malware.ru

[7] Результаты теста проактивной антивирусной защиты (декабрь 2007) — Тесты и сравнения антивирусов — Anti-Malware.ru

[8] Результаты теста антивирусов на обнаружение современных полиморфных вирусов — Тесты и сравнения антивирусов — Anti-Malware.ru

[9] Результаты теста антивирусов на быстродействие, рейтинги антивирусов по скорости работы (август 2008) — Тесты и сравнения антивирусов — Anti-Malware.ru

[10] Результаты теста самозащиты антивирусов (август 2007) — Тесты и сравнения антивирусов — Anti-Malware.ru

[11] Результаты теста самозащиты антивирусов (январь 2009) — Тесты и сравнения антивирусов — Anti-Malware.ru

[12] Результаты теста проактивной антивирусной защиты (март 2009) — Тесты и сравнения антивирусов — Anti-Malware.ru

[13] Тест антивирусов на защиту от новейших (Zero-day) вирусов, троянов, шпионских программ — результаты(ноябрь 2009) — Тесты и сравнения антивирусов — Anti-Malware.ru

[14] Антивирус Касперского 2009 получил очередную максимальную оценку тестовой лаборатории AV-Comparatives

[15] Новый «Касперский» пообещал «не тормозить»

[16] Касперский тормозит? Это правда, но правда эта давно протухла.

[17] Результаты теста антивирусов на быстродействие (март 2012)

[18] Антивирус Касперского тормозит? Этот миф развенчан!

[19] Для отображения титров нужно нажать на название продукта. В версии 7.0 при этом надо удерживать нажатыми правую кнопку мыши и клавишу Ctrl, а начиная с 2009 (8.0) достаточно простого щелчка.

93.9. Ссылки

- Обзор антивируса Касперский 2013 **от FreeSofter.Ru**
- Домашняя страница Лаборатории Касперского
- Страница загрузки программы и документации
- Информация об Антивирусе Касперского на сайте Лаборатории Касперского

- Список приложений, несовместимых с Антивирусом Касперского 2010
- Список программ, несовместимых с Антивирусом Касперского 2011
- Настройка Kaspersky Internet Security 2012
- Как настроить Антивирус Kaspersky CRYSTAL
- Как защитится от WinLock при помощи Kaspersky Internet Security
- *Дарья Куликова.* Обзор программы Kaspersky Anti-Virus 2011. SoftSalad.ru (17 января 2011). Архивировано из первоисточника 12 марта 2012.

Глава 94

ВирусБлокАда

ВирусБлокАда (**VBA32**) — антивирусное программное обеспечение, разработанное и развивающееся одноимённой белорусской компанией. Программа способна выявлять и обезвреживать вредоносный код в приложениях, в почтовой корреспонденции и в архивах. Распространяется бесплатно в виде пробной версии, все функции программы доступны только в платной версии.

94.1. Системные требования

Программа способна работать под управлением операционных систем семейства Windows: Windows 2000 (SP4 и выше), XP (SP2 и выше), XP Professional x64, Vista, W7 (поддерживаются как 32-, так и 64-битные версии), ей требуется процессор частотой от 300 МГц (рекомендуется от 800 МГц), 128 Мбайт ОЗУ (рекомендуется 512 Мбайт) и 50 Мбайт свободного места на жёстком диске для самой программы и 300 Мбайт для антивирусных баз.

94.2. Функции

Программа обеспечивает как проверку программ, так и архивов. Поддержана обработка и удаление вредоносного содержимого в почтовых сообщений на базах Microsoft Outlook Express, Microsoft Outlook, The Bat!. Антивирусные базы автоматически обновляются через Интернет, обновление программы не требует перезагрузки.

В программу включён эвристический анализатор, а также заявлена особая технология выявления вирусов. Разработчиками также отмечается встроенный в программу эмулятор процессора с динамической трансляцией кода, обрабатывающий полиморфные, упакованные и зашифрованные вирусы, используется в распаковщике исполняемых файлов, обработанных программами защиты кода от исследования и программами-упаковщиками.

94.3. Области применения

Разработчики рекомендуют применять программу как на персональных компьютерах и рабочих станциях, так и на интернет-шлюзах, файловых и почтовых серверах, в том числе под управлением UNIX-систем. Центр Управления Vba32 с веб-интерфейсом позволяет организовать централизованное управление и сбор статистики о работе антивирусного комплекса Vba32 на рабочих станциях как в локальной сети так и с множеством территориально распределенных отделений.

94.4. Критика

В тесте журнала Компьютерра от 2008 года указано, что программа работает сравнительно медленно и нашла только 3115 из 3732 вирусов, подготовленных для теста.

94.5. Разработчик

ОДО «ВирусБлокАда» — белорусский разработчик антивирусного программного обеспечения, резидент парка высоких технологий с 6 декабря 2006 года. Компания основана в мае 1997 года.

94.6. Примечания

94.7. Ссылки

- Официальный сайт для белорусских пользователей
- Vba32 User Guide
- *Крупин, Андрей* Малоизвестные бойцы цифрового фронта (рус.). Компьютерра (2 октября 2008). Проверено 11 июля 2011.

Глава 95

Лжеантивирус

Лжеантиви́рус (или **псевдоантивирус**) — компьютерная программа, которая имитирует удаление вредоносного программного обеспечения путём изначального заражения файлов компьютера-жертвы определённым вирусом.[1] К концу 2000-х годов значимость лжеантивирусов как угрозы персональным компьютерам снизилась.[2] В первую очередь, это связано с тем, что в США частично взяли под контроль индустрию spyware и adware[3], а UAC и антивирусы оставляют всё меньше шансов ПО, проникающему без ведома пользователя. Во-вторых, полноценных антивирусных программ стало настолько много, что сложно запомнить их все. Так, VirusTotal на конец 2015 года располагает 57 антивирусами.[4]

95.1. Описание и метод действия

Лжеантивирусы относятся к категории троянских программ[5], то есть программ-заразителей, распространяемых людьми с целью вымогательства банковских данных. В отличие от «нигерийских писем» (которые играют на алчности и сострадании), фишинга и ложных лотерейных выигрышей, лжеантивирусы похожи на винлокеры — они играют на страхе заражения системы[6], шантажируя пользователя для получения нужной информации. Встречаясь чаще всего под видом всплывающих окон веб-браузера, они якобы сканируют операционную систему пользователя и тут же выявляют в ней вирусы и другие вредоносные программы[2]. Для наибольшей достоверности, этот процесс также может сопровождаться внедрением одной или нескольких программ такого типа в систему путём обхода конфигурации[5], особенно если компьютер обладает минимальной и легкообходимой защитой. В итоге компьютер-жертва начинает выдавать сообщения о невозможности продолжения работы ввиду заражения, а лжеантивирус — упорно предлагать купить услугу или же разблокировать её, введя данные кредитной карты[7].

Самые первые лжеантивирусы возникли с развитием интернета и представляли собой лишь окна, имитирующие ОС (чаще всего — проводник Windows и рабочий стол интерфейса Windows XP) с присущими звуками при загрузке и нажатии кнопок. Такие окна легко убирались блокировщиками рекламы, например — Adblock Plus. Во второй половине 2000-х годов лжеантивирусы превратились в полноценные программы, и стали выдавать себя за настоящие антивирусы при помощи использования агрессивной рекламы, ложных пользовательских отзывов, или даже «отравления» поисковых результатов при вводе ключевых слов (в том числе по темам, не связанным с компьютерной безопасностью).[8][9][10] Такие программы задумывались с названиями, похожими на названия настоящих антивирусов (например *Security Essentials 2010* вместо «Microsoft Security Essentials» или *AntiVirus XP 2008* вместо «Norton AntiVirus») и работали по принципу прямого отправления денег распространителям — партнёрским сетям — за каждую удачную исталляцию.[11]

95.1.1. Статистика

В конце 2008 года обнаружили, что партнёрская сеть, распространявшая *Antivirus XP 2008*, получила за свою работу около 150 тыс. $.[12] В 2010 году Google пришёл к заключению, что половина вредоносного ПО, проникающего через рекламу, — лжеантивирусы.[13] В 2011 тот же Google исключил из поиска домен co.cc, дешёвый хостинг,[14] который облюбовали в том числе и распространители псевдоантивирусов. Специалисты из BitDefender в 2011 году обнаружили неординарного троянца. Хоть он и не является лжеантивирусом в обычном смысле, он распознаёт 16 обычных антивирусов, деинсталлирует их и заменяет имитацией.[15]

95.2. Выгода для распространителя

Распространитель может получать прибыль от лжеантивируса разными путями.

- Обычное для вредоносной программы по-

ведение: кража аккаунтов, блокировка ОС, эксплуатация вычислительной мощи компьютера и т. п.

- Программа может в «демонстрационном режиме» имитировать обнаружение вирусов и выдавать предупреждения о том, что ОС не защищена, а для исправления попросить зарегистрировать.[16][17] Чтобы была видимость заражения, лжеантивирус может устанавливать настоящие вирусы, а затем находить их, искусственно дестабилизировать ОС, изменяя критические настройки, и даже имитировать «синие экраны».[2]
- Лжеантивирус может просить деньги на псевдоблаготворительность.[18]
- Антивирусная программа может быть самая настоящая (обычно основанная на ClamAV), однако её цена, как правило, выше, чем цены на аналоги. Продают лицензию обычно поквартально — чтобы сравнить цены, приходится вчитываться в условия и подключать арифметику.

95.3. Простейшие признаки лжеантивируса

95.3.1. Сайт

- Лечение или демонстрация через веб.[19][20] Лечение через веб невозможно: веб-браузеры устроены так, чтобы сайт вообще не имел доступа к лежащим на компьютере файлам. А эффективность антивируса никак не коррелирует с красотой интерфейса.
- Большое количество несуществующих наград.[20]
- Настоящий антивирус не может гарантировать «стопроцентное излечение». Вирус должен попасться «в диком виде», кто-то из интернет-активистов отсылает его антивирусным специалистам, те исследуют его — и только после этого вирус попадает в базу. На это нужно время.
- «Крючки» в лицензионном соглашении: либо это «развлекательная программа», либо оплата идёт за «техподдержку ClamAV».[20]
- Оплата через SMS. Легальные антивирусы предпочитают платёжные системы и банковские карты.[20]

95.3.2. Программа

- Маленький размер инсталлятора или нет фазы инсталляции.[20] Dr. Web CureIt занимает более 100 мегабайт, аналогичная версия антивируса Касперского — около 150. У некоторых антивирусов (например, Avast!) бывает миниатюрный интернет-инсталлятор, но тогда все эти мегабайты будут скачаны из интернета во время установки.
- Срабатывает на «чистой» ОС, установленной с нуля,[20] обнаруживает не характерные для данной ОС вирусы (вирус, распространяющийся в Windows, выявляется для Linux).
- Окно UAC жёлтое (неподписанная программа), или синее, но владелец неверный (утёкший ключ).
- Если вы единственный администратор компьютера — программа, которую вы не устанавливали. Впрочем, утилиты поменьше, связанные с производительностью и безопасностью (например, чистильщики реестра) иногда распространяются «в придачу».
- Уже простейшая функциональность платная, без всяких испытательных периодов и бесплатных версий.[20] Например, у Лаборатории Касперского есть бесплатные варианты антивируса — *Kaspersky AVP Tool* и *Kaspersky Rescue Disk*. Деньги просят за дополнительные функции: брандмауэр, резидентный монитор, оперативное обновление и т. д.
- Навязчивые сообщения о том, что компьютер уязвим или нужно купить программу — а чаще всего то и другое одновременно.[20]
- Могут отсутствовать простейшие функции, присущие любой уважающей себя резидентной программе: временно остановить антивирус, деинсталлировать программу стандартными средствами ОС.[20] Может не быть и других настроек, присущих настоящему антивирусу (прокси-серверы, списки исключений).[20]

95.4. Примечания

[1] Symantec Report on Rogue Security Software. Symantec (28 октября 2009). Проверено 15 апреля 2010. Архивировано из первоисточника 13 августа 2012.

[2] Microsoft Security Intelligence Report volume 6 (July - December 2008) 92. Microsoft (8 апреля 2009). Проверено 2 мая 2009. Архивировано из первоисточника 13 августа 2012.

[3] *Leyden, John* Zango goes titsup: End of desktop adware market. The Register (11 апреля 2009). Проверено 5 мая 2009. Архивировано из первоисточника 13 августа 2012.

[4] Результат сканирования opensource-хука клавиатуры, который был использован в кейлоггере.

[5] Doshi, Nishant (2009-01-19), *«Misleading Applications – Show Me The Money!»*, Symantec, <https://forums2.symantec.com/t5/blogs/blogprintpage/blog-id/security_risks/article-id/53>. Проверено 2 мая 2009.

[6] The Perfect Scam — Technology Review

[7] News Adobe Reader and Acrobat Vulnerability. blogs.adobe.com. Проверено 25 ноября 2010. Архивировано из первоисточника 13 августа 2012.

[8] Chu, Kian & Hong, Choon (2009-09-30), *«Samoa Earthquake News Leads To Rogue AV»*, F-Secure, <http://www.f-secure.com/weblog/archives/00001779.html>. Проверено 16 января 2010.

[9] Hines, Matthew (2009-10-08), *«Malware Distributors Mastering News SEO»*, eWeek, <http://securitywatch.eweek.com/seo/malware_distributors_mastering_news_seo.html>. Проверено 16 января 2010.

[10] Raywood, Dan (2010-01-15), *«Rogue anti-virus prevalent on links that relate to Haiti earthquake, as donors encouraged to look carefully for genuine sites»*, SC Magazine, <http://www.scmagazineuk.com/rogue-anti-virus-prevalent-on-links-that-relate-to-haiti-earthquake-as-donors-encouraged-to-look-carefully-for-genuine-sites/article/161431/>. Проверено 16 января 2010.

[11] Doshi, Nishant (2009-01-27), *«Misleading Applications – Show Me The Money! (Part 3)»*, Symantec, <https://forums2.symantec.com/t5/blogs/blogprintpage/blog-id/security_risks/article-id/55>. Проверено 2 мая 2009.

[12] Stewart, Joe (2008-10-22), *«Rogue Antivirus Dissected - Part 2»*, SecureWorks, <http://www.secureworks.com/research/threats/rogue-antivirus-part-2/?threat=rogue-antivirus-part-2>

[13] Moheeb Abu Rajab and Luca Ballard (2010-04-13). «The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution» (Google). Проверено 2010-11-18.

[14] Google забанил домены .CO.CC | http://info.nic.ru

[15] Лжеантивирус-хамелеон - Securelist

[16] *«"Free Security Scan" Could Cost Time and Money»*, Federal Trade Commission, 2008-12-10, <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt121.shtm>. Проверено 2 мая 2009.

[17] SAP at a crossroads after losing $1.3B verdict. Yahoo! News (24 November 2010). Проверено 25 ноября 2010. Архивировано из первоисточника 13 августа 2012.

[18] CanTalkTech — Fake Green AV disguises as security software with a cause

[19] Хотя сервисы онлайн-сканирования существуют (например, VirusTotal), они не предлагают сканирования дисков локального компьютера, а требуют явной отправки подозрительного файла на проверку. Проверка, как правило, идёт несколькими широко известными антивирусами.

[20] Лаборатория Касперского о лжеантивирусах

95.5. Ссылки

- Howes, Eric L (2007-05-04), *«Spyware Warrior: Rogue/Suspect Anti-Spyware Products & Web Sites»*, <http://www.spywarewarrior.com/rogue_anti-spyware.htm>. Проверено 2 мая 2009.
- *«(en) List_of_rogue_security_software»*, <https://en.wikipedia.org/wiki/List_of_rogue_security_software>
- *«Kaspersky Lab: Rogue security software»*, <http://support.kaspersky.ru/viruses/rogue>. Проверено 24 апреля 2012.

Глава 96

Ревизор (программа)

Ревизо́р (от лат. *revisor* — пересматривающий; ср. лат. *revisio* — пересмотр) — компьютерная программа, запоминающая состояние компьютера, следящая за изменениями файловой системы и сообщающая о важных или подозрительных изменениях пользователю.

96.1. Принцип работы ревизоров

Программа-ревизор следит за изменениями файлов на компьютере. Для этого не обязательно делать копии всех файлов. Достаточно запомнить названия файлов и папок, размеры файлов и их контрольные суммы (либо специальные хеш-функции). Эта информация занимает немного места на диске, но позволяет заметить изменение любого файла. Периодически (по расписанию) или по приказу пользователя ревизор проверяет текущее состояние файловой системы и сравнивает с прежним. О подозрительных изменениях немедленно сообщается, об остальных пользователь может узнать при желании.

96.2. Назначение ревизоров

96.2.1. Антивирусное средство

Программы-ревизоры изначально предназначались для использования в качестве антивирусов. Любой вирус каким-либо образом изменяет систему данных на диске. Например, могут появиться новые исполняемые файлы, измениться уже существующие, может появиться сектор на диске, не связанный с каким-либо файлом и т. д. При обнаружении подозрительных изменений ревизор бьёт тревогу.

Достоинствами ревизоров как антивирусов являются:

- Быстрота проверки. В отличие от сканеров, которые должны содержимое файлов сверить с тысячами известных вирусных сигнатур, «на лету» разархивировать архивы, распаковать упакованные исполняемые файлы и библиотеки, ревизор подсчитывает лишь контрольную сумму. Это даёт экономию времени в десятки раз.
- Выявление любых новых вирусов. Если вирус отсутствует в базе данных (еще не занесён в базу или у данного пользователя устаревшая база), то сканер обычно не замечает вирус. Но любой вирус изменяет систему данных на диске, следовательно, выявляется ревизором.
- Возможность восстановления некоторых испорченных и уничтоженных файлов, а также лечения некоторых файлов, заражённых неизвестными вирусами. Обычные сканеры могут лечить лишь файлы, заражённые известными вирусами. Ревизоры сохраняют копии коротких файлов, наиболее важных файлов и файлов, чаще всего становящихся жертвами вирусов.

Ревизоры не в состоянии защитить компьютер от всех угроз со стороны вредоносного программного обеспечения, поэтому они обычно используются в комплексе с другими антивирусными средствами (например, при получении сигнала тревоги от ревизора запускается сканер).

96.2.2. Многопользовательские компьютеры

Если одним компьютером может пользоваться более одного человека, то возникает необходимость в контроле. Некоторые пользователи могут совершать запрещенные действия (устанавливать игры, сборщики паролей, взламывать систему, захламлять диск фильмами, музыкой, изображениями, изменять настройки и т. д.). Ревизоры могут выявлять эти действия, а также возвращать систему в нормальное состояние, не откатывая полезных изменений.

96.2.3. Другие применения

С помощью ревизора пользователи могут решать и другие проблемы: найти переименованный файл ли-

бо файл с забытым названием, выяснить причину сильно уменьшившегося свободного пространства на диске и т. д.

96.3. Российские программы

Из российских программ наиболее известны AdInf (Advanced Diskinfoscope) и ревизор, встроенный в антивирус Касперского.

Глава 97

Резидентная защита

Резиде́нтная защи́та — компонент антивирусного программного обеспечения, находящийся в оперативной памяти компьютера и сканирующий в режиме реального времени все файлы, с которыми осуществляется взаимодействие пользователя, операционной системы или других программ.

Слово «резидентный» означает «невидимый», «фоновый». Резидентный сторож (другое, более разговорное название этого вида защиты) проявляет себя только при нахождении вируса. Именно на резидентной защите основывается главный принцип антивирусного ПО — предотвратить заражение компьютера. В её состав входят такие компоненты, как активная защита (сравнение антивирусных сигнатур со сканируемым файлом и выявление известного вируса) и проактивная защита.

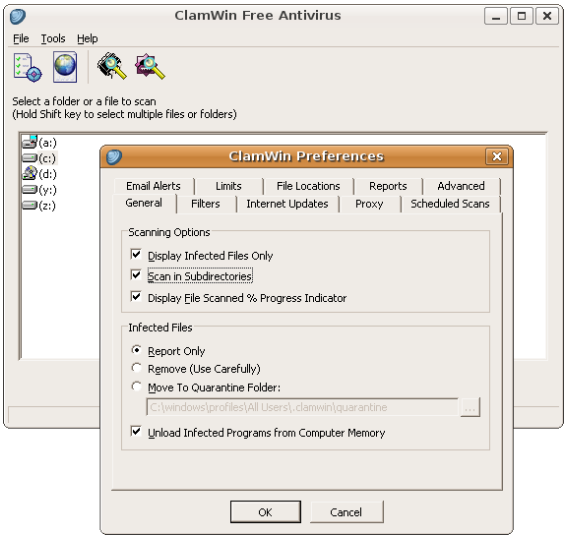
Резидентная защита — главный компонент любого антивирусного ПО.

97.1. См. также

- Антивирус
- Проактивная защита
- Эвристический анализатор

Глава 98

Clam Antivirus



ClamWin

Clam AntiVirus — пакет антивирусного ПО, работающий во многих операционных системах, включая Unix-подобные ОС, OpenVMS, Microsoft Windows и Apple Mac OS X.

Выпускается под GNU General Public License и является свободным программным обеспечением.

17 августа 2007 года проект ClamAV приобрела компания Sourcefire, производитель известной системы обнаружения вторжений Snort. По словам директора компании, Мартина Рауша, в ближайшее время продукты Snort и ClamAV будут объединены. Однако разработки ClamAV продолжат развиваться и предлагаться как отдельные бесплатные технологии.

Главная цель Clam AntiVirus — интеграция с серверами электронной почты для проверки файлов, прикреплённых к сообщениям. В пакет входит масштабируемый многопоточный демон clamd, управляемый из командной строки сканер clamscan, а также модуль обновления сигнатур по Интернету freshclam.

Возможности Clam AntiVirus:

- управление из командной строки;
- возможность использования с большинством почтовых серверов, включая реализацию milter-интерфейса для Sendmail;
- сканер в виде библиотеки Си;
- сканирование файлов и почты «на лету»;
- определение свыше 850 000 вирусов, червей, троянов, сообщений фишинга;
- анализ сжатых файлов RAR (2.0, 3.0), Zip, Gzip, Bzip2, MS OLE2, MS Cabinet, MS CHM (сжатый HTML) и MS SZDD;
- поддержка сканирования mbox, Maildir и «сырых» почтовых файлов;
- анализ файлов формата Portable Executable, упакованных UPX, FSG или Petite.

98.1. FrontEnd

- KlamAv — GUI для Clam AntiVirus в среде KDE.
- ClamTk — GUI для Clam AntiVirus в среде GNOME.

98.2. См. также

- ClamWin — Основанный на Clam AntiVirus антивирус для Windows
- Immunet — Ещё одна версия Clam AntiVirus для Windows. Текущая версия - 3.0.
- eShield Free Antivirus - Основанный на Clam AntiVirus антивирус для Windows, первая версия 1.1.0 появилась только в январе 2013 года, сейчас официальной версией считается 1.3.0.0
- Amiti Free Antivirus - Основанный на Clam AntiVirus антивирус для Windows, первая версия 1.0.195.0 появилась только в мае 2013 года. Выпускается фирмой из Словакии Netgate Technologies.

- AVITVA - еще один антивирус на движке ClamAV российского разработчика.
- ClamSentinel - свободный резидентный монитор для ClamAV.

98.3. Примечания

[1] ClamAV 0.99 has been released! (англ.). clamav.net (1 December 2015). Проверено 2 декабря 2015.

98.4. Ссылки

- Сайт проекта Clam AntiVirus
- Проект Clam AntiVirus на Sourceforge
- ClamAV онлайн
- Руководство пользователя Immunet Protect
- Видеообзор основных функций eShield Free Antivirus на русском языке.
- Видеообзор основных функций Amiti Antivirus на русском языке

Глава 99

ClamWin

ClamWin — свободный антивирусный сканер под Windows 98/ME/2000/XP/2003/Vista/7/8. Обеспечивает графический интерфейс к пакету Clam Antivirus.

ClamWin Free Antivirus выпускается под лицензией GNU General Public License и является свободным программным обеспечением. Поставляется с удобным инсталлятором (или portable) и исходными кодами.

Возможности ClamWin:

- Планировщик сканирования по расписанию.
- Автоматическое обновление антивирусной базы.
- Антивирусный сканер.
- Интеграция в контекстное меню Проводника в Windows.
- Плагин для Microsoft Outlook.
- Возможность работы с флэшки или компакт-диска без необходимости установки.

Также существует плагин для Mozilla Firefox, который может использовать ClamWin Free Antivirus для проверки скачиваемых файлов на вирусы [3].

99.1. Резидентное сканирование

В настоящее время ClamWin не может работать как антивирусный монитор (т.е. в режиме проверки всех запускаемые приложений на безопасность), возможности резидентного сканирования планируется добавить в следующих версиях, но существуют сторонние резидентные мониторы, такие как Clam Sentinel.

Программа WinPooch также позволяет использовать ClamWin в качестве резидентного сканера. Кроме этого она включает в себя функцию контроля сети.

99.2. Примечания

[1] Clamwin in Launchpad

[2] ClamWin Free Antivirus 0.98.7 Released

[3] Fireclam :: Add-ons for Firefox

99.3. Ссылки

- Резидентный движок-сканер Clam Sentinel 1.20
- Официальный сайт, русский раздел
- ClamWin на Sourceforge.net
- Antivirus Tools: Clam AV Is The Best — But Where Are The Rest?
- Проект WinPooch

Глава 100

WinPooch

Winpooch — это свободное программное обеспечение (лицензия GNU GPL), которое обнаруживает и удаляет spyware и некоторые виды троянов. Эта программа также обеспечивает резидентную защиту, используя сканеры ClamWin и BitDefender.

Разработка программы прекращена 13 июня 2008 года, согласно сообщению на странице программы на сайте Sourceforge. Официальный сайт уже не существует, но дистрибутив пока доступен на SourceForge.

100.1. Основные возможности программы

- Контроль над поведением программ (HIPS), включая:
  - Запуск и завершение программ.
  - Открытие файлов на чтение/запись.
  - Доступ к реестру Windows.
- Контроль сетевой активности приложений:
  - Открытие порта для прослушивания (то есть работа как сетевого сервера).
  - Подключение и передача данных программой к другому компьютеру.
- Резидентное сканирование и сканирование исполняемых программ, которые пытаются проделать контролируемые действия, используя встроенный или внешний антивирусный или антишпионский модуль.

Winpooch предлагает ряд возможностей по контролю за поведением программ, при этом пользователь может задействовать или отключать их, таким образом Winpooch можно использовать вместе с аналогичными другими программами — например, можно использовать встроенный файрвол Windows XP для контроля входящего трафика и Winpooch для исходящего трафика.

100.2. Ссылки

- Официальный сайт
- Проект WinPooch на сайте SourceForge.net

100.3. Источники текстов и изображения, авторы и лицензии

100.3.1. Текст

- **Ashampoo FireWall** *Источник:* https://ru.wikipedia.org/wiki/Ashampoo_FireWall?oldid=64273086 *Авторы:* BLISTHRV, PBot, Хитрый гнУс, MMH, WebCite Archiver, Programman, Well-Informed Optimist и Аноним: 2
- **AtGuard** *Источник:* https://ru.wikipedia.org/wiki/AtGuard?oldid=60853083 *Авторы:* Ctac, PBot, Wanderer777, ButkoBot, Peni, Yaroslav Blanter, РобоСтася, Whiteroll, U-bot, Addbot и Аноним: 3
- **Avast!** *Источник:* https://ru.wikipedia.org/wiki/Avast!?oldid=75313195 *Авторы:* APTEM, Softy, Roxis, A5b, Vlad2000Plus, V-17, Koterpillar, Putnik, Thijs!bot, BLISTHRV, Lockal, JAnDbot, PBot, Claymore, Gdn, AVRS, Alex Smotrov, Nick F0x, VolkovBot, Fnaq, Be nt all, Johnny Rotten, Vs64vs, SieBot, Flrn, Alexanderwdark, GrigorevMN, Mosn, Versageek, Макеенков Сергей, Zaqq, Bolshoy kot, Track13, Laim, Michaello, AnatoliyTkachev, AVB, Luckas-bot, Nallimbot, Tumkir, Rubinbot, Bootkiller, Obersachsebot, Xqbot, Partyzan XXI, Sabunero, DixonDBot, Sergeisemenoff, Man2~ruwiki, Суппилулиума, Абаддон, Xcell, EmausBot, Vajrapani, Stehenbeck, 6AND5, Википравитель, Зырты, LankLinkBot, TeachVideo Info, OneLittleMouse, ViglimBot, MGriBot, Excludeer, ChuispastonBot, H2Bot, Mjbmrbot, KrBot, Bugaevc, Shagrad, Владимир Шеляпин, Dima145, Евгений Геннадиевич Кушнырь, Hlynins, Rubinbot III, W2Bot, Vagobot, Sealle, AvocatoBot, Patrias, Razberum, Андрей Болтушкин, Well-Informed Optimist, Лукас Фокс, Болдинов Дмитрий, NightShadow23, Samuil19, Addbot, Starclyde, Arianneperrier, WalkDark и Аноним: 119
- **AVG** *Источник:* https://ru.wikipedia.org/wiki/AVG?oldid=74020801 *Авторы:* Robbot, Roboto de Ajvol, Roxis, Владимир Волохонский, AKA MBG, Cheops, A5b, MTrukhmanov, Putnik, ZsergheiBot, McLinker, Thijs!bot, BLISTHRV, JAnDbot, PBot, Gdn, CommonsDelinker, AVRS, Rmn, VolkovBot, Neo973, Aleksandrit, ButkoBot, TXiKiBoT, Holop, RusRec13, Loveless, NBS, AlleborgoBot, VVVBot, ???? robot, DragonBot, Pascal65536, Zeo, Alexbot, GreenStork, DerNews, MelancholieBot, Zorrobot, AnatoliyTkachev, Forajump, Amirobot, AVB, Luckas-bot, Alberth2, Ptbotgourou, Rubinbot, Mark Ekimov, MaxMax, ArthurBot, Misi91, Okras, DSisyphBot, Xqbot, SassoBot, IMnement, RedBot, Nogin, KamikazeBot, Small Bug, Artem Samarin, Amychok, TjBot, Ripchip Bot, EmausBot, Arbnos, MMH, ChuispastonBot, WikitanvirBot, Mjbmrbot, SloggerFox, Vladikas, KrBot, B.konjaria, MerlIwBot, KPu3uC B Poccuu, Usper, Patrias, Ilya Vorobev, Alexander128, Itshaman, Addbot, Oleg3280, Apacersis, Oro6kron, Antoha6996 и Аноним: 50
- **Avira Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Avira_Antivirus?oldid=75040454 *Авторы:* Korolev Alexandr, Roxis, Exile~ruwiki, Teufel, Infovarius, Escarbot, BLISTHRV, JAnDbot, PBot, Gdn, VolkovBot, TXiKiBoT, Peni, Viplux, Alexanderwdark, Analyzer (KODEP), Шмидт Владимир, Cofeman, Qldor, Abiyoyo, AnatoliyTkachev, Amirobot, MystBot, Ptbotgourou, JackieBot, Obersachsebot, MaxVT, Kaban2009, Partyzan XXI, Ch egor, EmausBot, Goldvarg, Vova Solomatin, Википравитель, Dmitry002, LankLinkBot, WikitanvirBot, WebCite Archiver, AviraFans, Fromsibir2008, Well-Informed Optimist, Andiorahn, Alexander128, Alan, Блокнот, Addbot, Retro-redakteur.u12 и Аноним: 45
- **BWMeter** *Источник:* https://ru.wikipedia.org/wiki/BWMeter?oldid=72562051 *Авторы:* PBot, Arg.amx, РобоСтася, U-bot, Vort, WebCite Archiver, Well-Informed Optimist и Аноним: 4
- **Cisco ASA** *Источник:* https://ru.wikipedia.org/wiki/Cisco_ASA?oldid=71455195 *Авторы:* Alex krylov, РобоСтася, U-bot, Nadenko, Намелесс, Dmbaturin, OneLittleMouse, KrBot, WebCite Archiver, MerlIwBot, Dulat K, Ascola, Robiteria и Аноним: 6
- **Comodo Firewall** *Источник:* https://ru.wikipedia.org/wiki/Comodo_Firewall?oldid=63333568 *Авторы:* Gruznov, Dstary, BLISTHRV, PBot, Gdn, Knyf, VolkovBot, Smolov.ilya, Malek, Andzaytsev, Che13, Vlsergey, Analyzer (KODEP), Tirthika, Ost., Eraser XB, Kinka, Pessimist2006, A4F, Dima-s93, Ghuron, D'ohBot, WindBot, Partyzan XXI, Killerbot, Sergeisemenoff, ArchoNotron, Alexander Roumega, LankLinkBot, SpaceRu, Bot89, Patrias, Well-Informed Optimist, Comodo Russia, СПЕцредаКТоР и Аноним: 31
- **Comodo Internet Security** *Источник:* https://ru.wikipedia.org/wiki/Comodo_Internet_Security?oldid=70864752 *Авторы:* Wind, JukoFF, Putnik, BLISTHRV, PBot, Knyf, VolkovBot, ButkoBot, TXiKiBoT, Vs64vs, Vlsergey, Analyzer (KODEP), SilvonenBot, РобоСтася, XClear, DSisyphBot, Xqbot, Dima-s93, Salamatiqus, X7q, Groovenstein, Partyzan XXI, Distdev, Ботильда, Sabunero, TobeBot, Sergeisemenoff, ArchoNotron, Artem Samarin, Amychok, LankLinkBot, H2Bot, Cinemantique, KrBot, Azag-Thoth, SpaceRu, MerlIwBot, KLBot2, KPu3uC B Poccuu, Bot89, Bondaruk85, Странный Странник, Well-Informed Optimist, Alexxsun, Andiorahn, Alexander128, IdeaMan, Васили и Аноним: 50
- **Deep packet inspection** *Источник:* https://ru.wikipedia.org/wiki/Deep_packet_inspection?oldid=73525188 *Авторы:* A5b, Youngfather, Vlsergey, Pessimist2006, Филатов Алексей, Rubinbot, Gromolyak, Dsund, AEffect, EmausBot, MGriBot, KrBot, Atmega644, Jackch~ruwiki, Zyamilon, MatrixRnd и Аноним: 17
- **Fortinet** *Источник:* https://ru.wikipedia.org/wiki/Fortinet?oldid=75413566 *Авторы:* Galliat, Deinocheirus, Rubinbot, Okras, WinterheartBot, Шуфель, Drakosh, MBHbot, RasabJacek, Robiteria, Bloodyritual, EvRubot, Ilrond и Аноним: 3
- **Ideco ICS** *Источник:* https://ru.wikipedia.org/wiki/Ideco_ICS?oldid=74496200 *Авторы:* PBot, CommonsDelinker, Alex Smotrov, Peni, Vlsergey, Burivykh, Netch, АлександрВв, Vort, Webzest, MotnahpBot, Da voli, LankLinkBot, OneLittleMouse, MBHbot, V.metikov, Анастасия Глебова, Glebaz, Доброжелатель и Аноним: 14
- **Ipchains** *Источник:* https://ru.wikipedia.org/wiki/Ipchains?oldid=74166304 *Авторы:* JukoFF, A5b, PBot, ArthurBot, U-bot, DenisKrivosheev, A.steklov, EmausBot, HRoestBot, Игорь Темиров, WebCite Archiver, MBHbot и Аноним: 2
- **IPFilter** *Источник:* https://ru.wikipedia.org/wiki/IPFilter?oldid=73506192 *Авторы:* Softy, Shattered, Веон, BLISTHRV, SieBot, Luckas-bot, JackieBot, Obersachsebot, DenisKrivosheev, Garrymaren, Dulat K, Addbot и Аноним: 2
- **IPFire** *Источник:* https://ru.wikipedia.org/wiki/IPFire?oldid=72319549 *Авторы:* Rubinbot, KrBot, RemiZOffAlex и Аноним: 5
- **Ipfw** *Источник:* https://ru.wikipedia.org/wiki/Ipfw?oldid=70090160 *Авторы:* A.I., Softy, Guzenkov, BLISTHRV, PBot, Claymore, VolkovBot, Важнов Алексей Геннадьевич, Holop, Bff7755a, Luckas-bot, Teox, Imroot, Leti wikiuser01, Karpion, Leti wikiuser02, Leti wikiuser03, Xaker1, D'ohBot, Sergguha, MondalorBot, EleferenBot, Deepak-nsk, Dutchman ru, WebCite Archiver, Dtulyakov, Addbot и Аноним: 16
- **Iptables** *Источник:* https://ru.wikipedia.org/wiki/Iptables?oldid=75209349 *Авторы:* Tetromino, Antono Vasiljev, Roxis, Cheops, A5b, Leksey, BLISTHRV, JAnDbot, PBot, AVRS, Rett Pop, Salmin, Alex Smotrov, Be nt all, Vs64vs, Sergey Spatar, Holop, IGx, Xaionaro, Xsfx, HORD, Томми Нёрд, Четыре тильды, Zealotous, Durman4eg, РобоСтася, Anarchim, Potekhin, Vpetrykanyn, Lucas

Novokuznetsk, ArtemBlack, Cuaxdon, Korobeynikov, Erud, Iluvatar, AVB, SF007, Jengelh, Tumkir, Sergrpd, Yodal, Shasha1, MaxMax, Рамиль Миннигалиев, Nokta strigo, Viglim, GreenGhost, AlexanderChemeris, Ботильда, Nnz1024, Palladium.security, EmausBot, Amblnb, Deepak-nsk, VIbot, 985D83E8, Piotryy293, Macumazan, Tlbycn, OneLittleMouse, Ibn.Card1nal, Tufex, LarBot, ViglimBot, Pravoslav, H2Bot, Radioxoma, WikitanvirBot, Keyboardman, PtQa, MerlIwBot, MBHbot, Extern, Coolmans, Addbot, Olzirg, Swssnif, !болит и Аноним: 83

- **Jetico Personal Firewall** *Источник:* https://ru.wikipedia.org/wiki/Jetico_Personal_Firewall?oldid=67933618 *Авторы:* PBot, Alex.ryazantsev, Skip01, EmausBot, H2Bot, Movses-bot, MBHbot, Wanhallen и Аноним: 2
- **Kaspersky Internet Security** *Источник:* https://ru.wikipedia.org/wiki/Kaspersky_Internet_Security?oldid=75259032 *Авторы:* Torin, Ilana, Obersachse, APTEM, Roxis, Incnis Mrsi, Sasha Krotov, AndyVolykhov, Vlad2000Plus, DR, Igor503, Stansult, Insider, Putnik, BLISTHRV, PBot, Gdn, CommonsDelinker, Jazz, Alex Smotrov, Kalan, Aleksandrit, Sonik, Holop, Int ft, Peni, Alexanderwdark, Iakov, Botinko, Agent001, Dmitry Rozhkov, Grebenkov, Timag~ruwiki, Eleferen, BloodyRose, GreenStork, Artiyom, Kinka, Lucas Novokuznetsk, Laim, Kvorum, Abiyoyo, AVB, Евгений Малинин, Lunar stranger, Tumkir, VOVANBFG, Fanni 93, MiStr, The-Twister, Aglu, Partyzan XXI, Щербина, Pirockar, Distdev, MASolomko, Dimashome, TheSLY, Sabunero, Prowdtobegeek, NeoCreator, Demon177, BOOMER 74, Spawnsony, MotnahpBot, Drakosh, Konjernb, Vomiting, Panchomoscow, Синкретик, LankLinkBot, OneLittleMouse, Tracker, Paulobazini, Викимонетчик, Mr.Simbir, LordRimmon, Джек Воробей, Movses-bot, WebCite Archiver, MarShaLL22, MerlIwBot, FaustGT, Apal0n, MBHbot, Programman, Nikiror, Андрей Болтушкин, Well-Informed Optimist, Volovik Vitaly, Alexxsun, I.G.I.cool, Mops nonna, Zakananis и Аноним: 112
- **Kerio Control** *Источник:* https://ru.wikipedia.org/wiki/Kerio_Control?oldid=72667289 *Авторы:* Cheops, PBot, Vicpeters, Ru wiki, Alex.ryazantsev, UncleMartin, Lucas Novokuznetsk, Pemu, Sergeisemenoff, Dinamik-bot, EmausBot, Omicrown, OneLittleMouse, KrBot и Аноним: 16
- **L7-filter** *Источник:* https://ru.wikipedia.org/wiki/L7-filter?oldid=71084354 *Авторы:* Переход Артур, CommonsDelinker, Peni, U-bot, Archer Godson, Mutari-Dirk, ViglimBot, KPu3uC B Poccuu, Addbot и Аноним: 2
- **Little Snitch** *Источник:* https://ru.wikipedia.org/wiki/Little_Snitch?oldid=73554757 *Авторы:* PBot, Sonik, Искандер2К, Manjel, Classic™, H2Bot, KrBot, Addbot и Аноним: 2
- **Microsoft Forefront Threat Management Gateway** *Источник:* https://ru.wikipedia.org/wiki/Microsoft_Forefront_Threat_Management_Gateway?oldid=73270147 *Авторы:* Softy, Volkov, A5b, Yaleks, AntonR, BLISTHRV, VolkovBot, VVVBot-temp, SieBot, Peni, Loveless, WikiCle, Svin0, FreeBSP, □□□□ robot, PixelBot, Potekhin, Lucas Novokuznetsk, Archishenok, Zorrobot, LaaknorBot, Rubinbot, Obersachsebot, Xqbot, Rusmuzhik, Partyzan XXI, Ch egor, Gayevoy, Pms1211, Valeriy.L, Игорь Темиров, FILbot, WikitanvirBot, WebCite Archiver, AvocatoBot, Addbot и Аноним: 27
- **Netfilter** *Источник:* https://ru.wikipedia.org/wiki/Netfilter?oldid=74872903 *Авторы:* Tetromino, Obersachse, Ilya Voyager, Shattered, Leksey, Koterpillar, BLISTHRV, JAnDbot, PBot, Sergey371, AVRS, Rett Pop, Rei-bot, DmitTrix, Mcherenkov, Alex.ryazantsev, Urutseg, IGx, Томми Нёрд, BMan, PixelBot, Plashchynski, OKBot, Bitobor, Norrius, РобоСтася, Jengelh, Rubinbot, MaxMax, Garrymaren, Ботильда, Mutari-Dirk, Deepak-nsk, Tlbycn, Wi user, WebCite Archiver, MerlIwBot, Addbot, ScotXW, Bodrych и Аноним: 10
- **Norton 360** *Источник:* https://ru.wikipedia.org/wiki/Norton_360?oldid=72295832 *Авторы:* Obersachse, Bezik, Incnis Mrsi, Strategе, George Shuklin, Escarbot, MadDog, BLISTHRV, PBot, ButkoBot, Berserkerus, Peni, Loveless, Голем, Lion.ua, VVVBot, Darkicebot, РобоСтася, Potekhin, Zorrobot, Muro Bot, AmphBot, LaaknorBot, AVB, Rubinbot, Jotterbot, Xqbot, Kaban2009, APTEM9309, EmausBot, WikitanvirBot, WebCite Archiver, Ltanner2, Symantec-Ru, Facenapalm и Аноним: 19
- **Norton Internet Security** *Источник:* https://ru.wikipedia.org/wiki/Norton_Internet_Security?oldid=72040071 *Авторы:* Bezik, Escarbot, PBot, Peni, Potekhin, Lucas Novokuznetsk, Muro Bot, Rubinbot, Jotterbot, Kaban2009, Alexey Izbyshev, Gizzatullin, Artem Samarin, APTEM9309, EmausBot, Василиса19, WikitanvirBot, Александр Русский, WebCite Archiver, Ltanner2, Patrias, Well-Informed Optimist, Trava152, Symantec-Ru, Артём гамаюнов владимирович, Addbot и Аноним: 22
- **NPF** *Источник:* https://ru.wikipedia.org/wiki/NPF?oldid=53782794 *Авторы:* Grayed, Luckas-bot, Obersachsebot, DenisKrivosheev, EmausBot и Аноним: 1
- **Online Armor** *Источник:* https://ru.wikipedia.org/wiki/Online_Armor?oldid=74642452 *Авторы:* Obersachse, Переход Артур, BLISTHRV, PBot, Claymore, AVRS, SieBot, Eraser XB, Qkowlew, GreatKir, Agel, Obersachsebot, Thrill, Xqbot, Ботильда, Sergeisemenoff, LankLinkBot, MarShaLL22, KPu3uC B Poccuu, Bot89, Well-Informed Optimist, Addbot и Аноним: 14
- **Outpost Firewall** *Источник:* https://ru.wikipedia.org/wiki/Outpost_Firewall?oldid=74871275 *Авторы:* Куллер, YurikBot, Stassats, Bezik, APTEM, CodeMonkBot, Volkov, Vlad2000Plus, BotCat, Edwardspec TalkBot, Александр Крайнов, Aml, Putnik, BLISTHRV, PBot, Gdn, V-yanko, MadMan, Rei-bot, NetSpiderUA, VolkovBot, Latitude, Fnaq, Redmond Barry, GrigorevMN, Kinka, Aqetz, Amirobot, Luckas-bot, Bootkiller, Gromolyak, AshikBot, D'ohBot, EmausBot, WikitanvirBot, AKIMOV09, Kapman~ruwiki, Kdm, Programman, Yagorman, Addbot, Pusto и Аноним: 22
- **Packet Filter** *Источник:* https://ru.wikipedia.org/wiki/Packet_Filter?oldid=74366294 *Авторы:* Softy, Roxis, Sir sigurd, Grain, Grayed, Itsme~ruwiki, BLISTHRV, Ya652ey, Важнов Алексей Геннадьевич, Lvova, VVVBot-temp, Loveless, VVVBot, Maedros, LA2-bot, PixelBot, Netch, VlsergeyBot, Ustas.SSR, Антон Касимов, Xqbot, DenisKrivosheev, KamikazeBot, H2Bot, WebCite Archiver, Dtulyakov, MBHbot, 762bot, Addbot и Аноним: 8
- **Panda Cloud Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Panda_Cloud_Antivirus?oldid=73245458 *Авторы:* Amikeco, BLISTHRV, PBot, Amirobot, RedBot, Krassotkin, EmausBot, Gamliel Fishkin, MMH, Deepak-nsk, ZéroBot, Tar-Mairon, WebCite Archiver, Patrias, Well-Informed Optimist, Itshaman и Аноним: 8
- **PC Tools Firewall Plus** *Источник:* https://ru.wikipedia.org/wiki/PC_Tools_Firewall_Plus?oldid=60853456 *Авторы:* BLISTHRV, PBot, Forajump, Rubinbot, Vort, RedBot, KamikazeBot, Well-Informed Optimist и Аноним: 2
- **PfSense** *Источник:* https://ru.wikipedia.org/wiki/PfSense?oldid=75022934 *Авторы:* TijAY, Alex.ryazantsev, Kravich, Ghuron, EmausBot, ZéroBot, OneLittleMouse, Movses-bot, Korob202, MBHbot, UnrealX6, GooDZon 999, BaseBot, Tessster, Olzirg, Dkgnim и Аноним: 25
- **Shorewall** *Источник:* https://ru.wikipedia.org/wiki/Shorewall?oldid=73835425 *Авторы:* Сибирский Лайка, BLISTHRV, PBot, РобоСтася, Luckas-bot, Rubinbot, Sealedend, Xqbot, LimeHat, Ole Førsten, Partyzan XXI, Artem Korzhimanov, Vort, Unikum111, EmausBot, LankLinkBot, ViglimBot, Addbot, Facenapalm, EvRubot и Аноним: 13

- **TMeter** *Источник:* https://ru.wikipedia.org/wiki/TMeter?oldid=69713308 *Авторы:* A5b, PBot, РобоСтася, U-bot, Ante, Panchomoscow, OneLittleMouse, Radioshark и Аноним: 5
- **Traffic Inspector** *Источник:* https://ru.wikipedia.org/wiki/Traffic_Inspector?oldid=75044096 *Авторы:* Melirius, Рулин, George Shuklin, PBot, Wanderer777, Renessaince, Obersachsebot, Kozeeva Yuliya, Mialgri, Drakosh, OneLittleMouse, Medova Tatyana, Movses-bot, MerlIwBot, MBHbot, Programman, Tatyana medova, Well-Informed Optimist, RotlinkBot и Аноним: 9
- **Uncomplicated Firewall** *Источник:* https://ru.wikipedia.org/wiki/Uncomplicated_Firewall?oldid=67096705 *Авторы:* PBot, DenisKrivosheev, DarkSTALKER, EmausBot, Astrum, Movses-bot и Аноним: 1
- **Zentyal** *Источник:* https://ru.wikipedia.org/wiki/Zentyal?oldid=69313011 *Авторы:* Nzeemin, Важнов Алексей Геннадьевич, Nik vr, Phoenix720, Structor, EmausBot, ZéroBot, Movses-bot, KrBot, WebCite Archiver, Dtulyakov, Olzirg и Аноним: 12
- **ZoneAlarm** *Источник:* https://ru.wikipedia.org/wiki/ZoneAlarm?oldid=74511346 *Авторы:* A5b, Vlom, BLISTHRV, PBot, Alex Spade, VolkovBot, Loveless, Yakiv Gluck, SergeyJ, Darkicebot, AlanNova, РобоСтася, Aquarius51, Lucas Novokuznetsk, SF007, ChenzwBot, Ботильда, Dinamik-bot, Xcell, Drakosh, WikitanvirBot, Dulat K, Patrias, Addbot и Аноним: 6
- **Брандмауэр Windows** *Источник:* https://ru.wikipedia.org/wiki/%D0%91%D1%80%D0%B0%D0%BD%D0%B4%D0%BC%D0%B0%D1%83%D1%8D%D1%80_Windows?oldid=75310210 *Авторы:* Obersachse, Cheops, DmitTrix, Jackie, SilvonenBot, Raegdan, Lucas Novokuznetsk, Rubinbot, Радион, Fanni 93, D'ohBot, MondalorBot, Ch egor, DixonDBot, Wform, Ivan-94, SEA99, Wikifido, WikitanvirBot, CAT Server, MerlIwBot, MBHbot, Луговкин, Geka b, Addbot, Oleg3280, Q-bit array и Аноним: 16
- **Интернет Контроль Сервер** *Источник:* https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C_%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80?oldid=74125057 *Авторы:* Torin, YurikBot, A5b, CommonsDelinker, Vlsergey, Bilderling, РобоСтася, Longbowman, Pessimist2006, U-bot, Ante, AbiyoyoBot, OneLittleMouse, El-chupanebrej, H2Bot, Movses-bot, KrBot, Sun4wind, Cemenarist, MBHbot, KPu3uC B Poccuu, Mustafaalmas, Луговкин, ZolPar, EvRubot, Alex NB IT и Аноним: 9
- **Интернет-шлюз** *Источник:* https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%88%D0%BB%D1%8E%D0%B7?oldid=71864519 *Авторы:* Obersachse, Cheops, Lite, ShinePhantom, Peni, 4epenOK, Petrov Victor, Сергеев Павел, LaaknorBot, Obersachsebot, Xqbot, MaksIv, Mixabest, Ll0l00l, Kuzyara, OneLittleMouse, Sun4wind, Bloodyritual, KrashVS, Addbot, KonstantinSer и Аноним: 22
- **Континент (программа)** *Источник:* https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%82%D0%B8%D0%BD%D0%B5%D0%BD%D1%82_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0)?oldid=71228678 *Авторы:* A5b, DonRumata, Peni, Yaroslav Blanter, РобоСтася, Rambalac, AVB, Rubinbot, D.bratchuk, Gabrealsafm, Msafronov, Da voli, 13243546A, KrBot, WebCite Archiver, TEXHNK77, MBHbot, Тара-Амингу и Аноним: 10
- **Межсетевой экран** *Источник:* https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD?oldid=75132720 *Авторы:* Robbot, Александр Сигачёв, Jaroslavleff, M5, Tetromino, Куллер, Skor, YurikBot, Bezik, Polzohod, LyXX, Wassily, Chobot, Roxis, Winterheart, Csman, A5b, Negrizprovod, SergeMukhin, C0der, Mercury, Maksim-bot, Alex Kassarin, Shattered, Mcusheff, Vlad2000Plus, George Shuklin, Illythr, Nikolay Nikolaevich Fedotov, Edwardspec TalkBot, Stansult, Grain, Glower, Busla, VPliousnine, Grayed, Escarbot, AntonR, ZserghеiBot, Thijs!bot, JAnDbot, Gdn, Yurikoles, Alex Smotrov, VolkovBot, Lew Wadoo, Idioma-bot, TXiKiBoT, Vs64vs, Walker~ruwiki, Newt, SieBot, YonaBot, Berserkerus, Loveless, NBS, AlleborgoBot, Vlsergey, Samal, Tomich, DragonBot, LA2-bot, Manslay, Mortiiz, PixelBot, Rights2Fly, BOTarate, XJIOP, Baturin, LatitudeBot, VlsergeyBot, Alecs.bot, Potekhin, Lucas Novokuznetsk, MelancholieBot, Laim, Amirobot, Luckas-bot, Azakhark, XClear, Obersachsebot, ArthurBot, 4th-otaku, Bublik 33007, Leti wikiuser01, Xqbot, Wcrazy, DenisKrivosheev, Maickellz, MastiBot, Dmbaturin, Partyzan XXI, Супприат, Vort, TobeBot, Enavt, Ver-bot, EmausBot, Drakosh, ????4, Tulmatsch, ZéroBot, HRoestBot, Tlbycn, Zero2525, Collateralinjures, RichKa, Ebrambot, WikitanvirBot, Movses-bot, MBHbot, VITAL105, Ascola, Андрей Бондарь, Justincheng12345-bot, Быченков, Kzi-manual, Quicktotal, Addbot, Martifik, Q-bit array и Аноним: 88
- **Персональный файрвол** *Источник:* https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%84%D0%B0%D0%B9%D1%80%D0%B2%D0%BE%D0%BB?oldid=74531293 *Авторы:* Roboto de Ajvol, Sasha Krotov, George Shuklin, Doomych, Bunker by, SieBot, Loveless, Rights2Fly, Нирваньчик, LatitudeBot, Potekhin, Lucas Novokuznetsk, Rubinbot, 4th-otaku, Xqbot, WindBot, Partyzan XXI, Rashevskiy, EmausBot, Drakosh, Tlbycn, Gipoza, Андрей Бондарь, Dexbot, Быченков, Addbot, Facenapalm и Аноним: 9
- **Сетевой шлюз** *Источник:* https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%88%D0%BB%D1%8E%D0%B7?oldid=70465853 *Авторы:* Vladimir Solovjev, Keeper B, JAnDbot, Alex.ryazantsev, Peni, Shlakoblock, Jukier, Myrzich Cyril, Alexbot, 4epenOK, Alecs.bot, Khelgar, Luckas-bot, Sergrpd, ArthurBot, Xqbot, Skab, Ole Førsten, Gweorth, EmausBot, ZéroBot, ChuispastonBot, WikitanvirBot, MerlIwBot, Sandyotic, Pinepain, Bloodyritual, Addbot, Elhefe и Аноним: 20
- **Антивирусная программа** *Источник:* https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0?oldid=75206494 *Авторы:* Maximaximax, Torin, Dodonov, Ornil, Obersachse, D12, Xchgall, YurikBot, Butko, SergV, Adrianopol, Gruznov, Palica, Zwobot, Talextk, Roxis, Csman, Volkov, JaroslavleffBot, Mercury, MaxSem, Sasha Krotov, Lite, Vlad2000Plus, The Wrong Man, Danvolodar, Avmaksimov, Y2y, Dstary, DR, Nikolay Nikolaevich Fedotov, Edwardspec TalkBot, Stansult, Putnik, IwanS, Thijs!bot, JAnDbot, Иван Тайга, Gdn, Temarez, Сергей Олегович, Knyf, Metalim, Alex Smotrov, DorganBot, VolkovBot, Anodonta, Vlad2000PlusBot, Wanderer777, Sicon, Idioma-bot, Askusnov, TXiKiBoT, Elmor, Vladimir Ivanov, FearChild, WXP, Mcherenkov, SieBot, Alex.ryazantsev, Peni, PolarBot, Vlsergey, Delog, David.s.kats, GrigorevMN, PipepBot, AlexanderD, Poit-ssv, HORD, ???? robot, DragonBot, Rights2Fly, OKBot, Petrov Victor, SolitaryDreamer, Ufim, Изумруд, SilvonenBot, VlsergeyBot, Alecs.bot, LynXzp, CarsracBot, AS, AnatoliyTkachev, AVB, Luckas-bot, Futball80, Bootkiller, Фил Вечеровский, Misi91, Renych, XZeroBot, Elfenit, Ramses, SassoBot, Saint-denis, Schekinov Alexey Victorovich, ChenzwBot, Андрей Евсеенко, Sigwald, AntonST, Marbi777, Partyzan XXI, MASolomko, Zuleg, Tmin10, Krassotkin, Rashevskiy, Convallaria majalis, Gayevoy, Mutari-Dirk, Laiquanaro, EmausBot, Y.barninets, Drakosh, Plakhow, HRoestBot, Helgi-S, Iron4eg, Hunex, Centurion198, LankLinkBot, OneLittleMouse, ChuispastonBot, H2Bot, Brateevsky, WikitanvirBot, Homk, Abc41, KrBot, Karachun, MerlIwBot, W2Bot, Александровская2731, Extern, Well-Informed Optimist, Наумов Андрей, Nikulina Julia, Alexxsun, Вячеслав9000, Andiorahn, Addbot, Tankograd174Rus, GEOgraf RUS, MrVirusHack, Q-bit array и Аноним: 237

- **Acronis AntiVirus** *Источник:* https://ru.wikipedia.org/wiki/Acronis_AntiVirus?oldid=69315987 *Авторы:* PBot, WXP, Luckas-bot, EmausBot, Arbnos, LankLinkBot и Аноним: 1
- **ActiveVirusShield** *Источник:* https://ru.wikipedia.org/wiki/ActiveVirusShield?oldid=68485434 *Авторы:* OckhamTheFox, Roxis, Koterpillar, Thijs!bot, BLISTHRV, PBot, Gdn, VolkovBot, DodekBot~ruwiki, VVVBot-temp, CheloVechek, Lockalbot, AnatoliyTkachev, AVB, Luckas-bot, Yu mor, HAL9000, LankLinkBot, Addbot, Tentatum и Аноним: 7
- **Advanced SystemCare** *Источник:* https://ru.wikipedia.org/wiki/Advanced_SystemCare?oldid=74789804 *Авторы:* PBot, CommonsDelinker, РобоСтася, Maks13, Tnktnp, EmausBot, Well-Informed Optimist, 6уKBa, WalkDark и Аноним: 6
- **Advanced SystemCare Ultimate** *Источник:* https://ru.wikipedia.org/wiki/Advanced_SystemCare_Ultimate?oldid=75425257 *Авторы:* PBot, РобоСтася, Maks13, MMH, Игорь Темиров, Well-Informed Optimist и Фёдор Кусков
- **Aidstest** *Источник:* https://ru.wikipedia.org/wiki/Aidstest?oldid=69227669 *Авторы:* Ctac, Obersachse, FHen, Shattered, BLISTHRV, PBot, Claymore, VolkovBot, Wanderer777, Redek, IvoryTower, Дмитрий Кошелев, РобоСтася, AVB, Rubinbot, Obersachsebot, Sokil.off, WindBot, Zoq-Fot-Pik, KrBot и Аноним: 2
- **Ashampoo AntiSpyWare** *Источник:* https://ru.wikipedia.org/wiki/Ashampoo_AntiSpyWare?oldid=64273057 *Авторы:* PBot, Хитрый гнУс, Exxxxxcel~ruwiki, WebCite Archiver, Programman, Well-Informed Optimist и Аноним: 3
- **Ashampoo AntiVirus** *Источник:* https://ru.wikipedia.org/wiki/Ashampoo_AntiVirus?oldid=70632551 *Авторы:* PBot, Petrov Victor, Хитрый гнУс, MMH, Exxxxxcel~ruwiki, WebCite Archiver, Programman и Аноним: 4
- **AVZ** *Источник:* https://ru.wikipedia.org/wiki/AVZ?oldid=73174095 *Авторы:* Obersachse, Antondr, Butko, Volkov, Elk Salmon, Алексей Скрипник, Dstary, Koterpillar, Altes, BLISTHRV, PBot, Gdn, Jazz, Nickispeaki, VolkovBot, FearChild, Mcherenkov, NBS, Yaroslav Blanter, Rubin16, РобоСтася, Lucas Novokuznetsk, Darkswarmzero, AVB, Rubinbot, Obersachsebot, 4th-otaku, Partyzan XXI, Vort, MMH, Panchomoscow, Leverimprovement, LankLinkBot, OneLittleMouse, WebCite Archiver, Артем Поминов, Addbot, Apacersis, Ffoxin и Аноним: 36
- **BitDefender** *Источник:* https://ru.wikipedia.org/wiki/BitDefender?oldid=72419906 *Авторы:* OckhamTheFox, Roxis, Arnasay, RuED, Escarbot, MIKE B2, ZsergheiBot, BLISTHRV, PBot, Gdn, CommonsDelinker, AVRS, Alex Smotrov, VolkovBot, Ashik, TXiKiBoT, SieBot, Loveless, GrigorevMN, VVVBot, Bobsky, Alexbot, UR3IRS, AnatoliyTkachev, Amirobot, AVB, Luckas-bot, Bootkiller, MusaAli, Obersachsebot, Xqbot, LucienBOT, Qazyi, TobeBot, EmausBot, ZéroBot, Tar-Mairon, Centurion198, HAL9000, ViglimBot, Dulat K, Patrias, Well-Informed Optimist, Trava152, Addbot, Facenapalm, Inscrutable man, Jullsy и Аноним: 28
- **BitDefender TrafficLight** *Источник:* https://ru.wikipedia.org/wiki/BitDefender_TrafficLight?oldid=65950518 *Авторы:* Terrible broom, АлександрВв, Deepak-nsk, Tar-Mairon, WebCite Archiver, RotlinkBot и Аноним: 3
- **Bullguard Internet Security** *Источник:* https://ru.wikipedia.org/wiki/Bullguard_Internet_Security?oldid=60961954 *Авторы:* WXP, Nter, РобоСтася, MystBot, Vikeke, EmausBot, LankLinkBot, WikitanvirBot, MerlIwBot, Trava152, Apacersis и Аноним: 2
- **CA Antivirus** *Источник:* https://ru.wikipedia.org/wiki/CA_Antivirus?oldid=58381083 *Авторы:* Bezik, Grebenkov, Синдар, Bopsulai, KrBot, Сапига Инна, Babalonius, EvRubot и Аноним: 3
- **Comodo Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Comodo_Antivirus?oldid=72694000 *Авторы:* JukoFF, Dstary, Chup, BLISTHRV, PBot, Nickispeaki, VasilievVV, VolkovBot, Peni, Vlsergey, Analyzer (KODEP), Pessimist2006, Dima-s93, D'ohBot, Partyzan XXI, Sergeisemenoff, ArchoNotron, Artyom K., BeZloR, W2Bot, Bot89, Well-Informed Optimist, Addbot, Apacersis, СПЕцредаКТоР и Аноним: 17
- **COMODO Cleaning Essentials** *Источник:* https://ru.wikipedia.org/wiki/COMODO_Cleaning_Essentials?oldid=63333877 *Авторы:* PBot, KrBot, Странный Странник, Well-Informed Optimist и Аноним: 3
- **Dr. Solomon's Anti-Virus Toolkit** *Источник:* https://ru.wikipedia.org/wiki/Dr._Solomon'{}s_Anti-Virus_Toolkit?oldid=53668449 *Авторы:* Obersachse, Peni, Jackie, U-bot, Vikeke, Gayevoy, Tockman, Addbot и Аноним: 1
- **Dr.Web** *Источник:* https://ru.wikipedia.org/wiki/Dr.Web?oldid=75385529 *Авторы:* Snch, Sergei Frolov, Al Silonov, OckhamTheFox, Roxis, Volkov, JaroslavleffBot, Морган, John~ruwiki, Lite, Vlad2000Plus, ЭфрониУри, Беломоев Алексей, Escarbot, BLISTHRV, Lockal, PBot, Gdn, Wybot, CommonsDelinker, Rps5, Rmn, Alex Smotrov, VolkovBot, Latitude, Arakcheev, Deerhunter, Aibot, TXiKiBoT, Wikiwide, A.Savin, Grisha1995, Elmor, RomanLeonov, Gum, Worrdo, ·1e0nid·, NBS, Vlsergey, Alexanderwdark, GrigorevMN, Starless, Четыре тильды, Petrov Victor, Kinka, Different.local, Mishka22, Laim, Kvorum, AnatoliyTkachev, LaaknorBot, AVB, Luckas-bot, Anton Polunin, Rubinbot, Bootkiller, WindEwriX, Obersachsebot, Dragon-zla, Ксения СПб, LimeHat, GAndy, DenisKrivosheev, Structor, LucienBOT, Maximkuk, Schrike, Major0709, DarkSTALKER, Mantyr, Vort, Bopsulai, Тимофей Конев, Segax, Zombiyaic, JenVan, Pms1211, Valdis72, Gamliel Fishkin, Mr.Aleksio, LASDORF, ShaVas, LankLinkBot, OneLittleMouse, Elchupanebrej, LarBot, Nohero, Wikifido, ChuispastonBot, H2Bot, Brateevsky, KrBot, WebCite Archiver, FaustGT, W2Bot, Барвенковский, MBHbot, Green Ivan, Programman, 91i79, Zubahistka, Well-Informed Optimist, Туманный сталкер, Dart Raiden, Папа рядом!, Sgt.koryavy, Addbot, Dudinroman, Apacersis, Dannko, Grakrus, Glovacki, TemirovBot, Drwebguy и Аноним: 112
- **Dr.Web Live CD** *Источник:* https://ru.wikipedia.org/wiki/Dr.Web_Live_CD?oldid=73221956 *Авторы:* ЭфрониУри, BotCat, PBot, Zimak, Wikiwide, Yaroslav Blanter, Starless, РобоСтася, AVB, Speckurshtml, Obersachsebot, Melksoft, U-bot, Викарий, LankLinkBot, W2Bot, DimaBot, IbraMLab и Аноним: 10
- **EICAR-Test-File** *Источник:* https://ru.wikipedia.org/wiki/EICAR-Test-File?oldid=74626062 *Авторы:* A5b, Mercury, Infovarius, Jeron, AVRS, VolkovBot, Peni, Musicien, РобоСтася, SpBot, Оззи, Obersachsebot, TobeBot, Википравитель, LankLinkBot, H2Bot, WikitanvirBot, Justincheng12345-bot, Addbot, Glovacki, LillySmithers и Аноним: 21
- **Emsisoft Anti-Malware** *Источник:* https://ru.wikipedia.org/wiki/Emsisoft_Anti-Malware?oldid=62949943 *Авторы:* Doomych, Shamin Roman, Chath, Yaroslav Blanter, АлександрВв, Luckas-bot, Compsyg, KamikazeBot, EmausBot, ZéroBot, MrFedikable, Martin Devil, Addbot, Bobrov Andrey и Аноним: 10
- **EScan Antivirus** *Источник:* https://ru.wikipedia.org/wiki/EScan_Antivirus?oldid=62678616 *Авторы:* KVK2005, Worrdo, AndreiK, Юрий Педаченко, KrBot, Любовь Шулупина, EScan, Apacersis и Аноним: 4
- **ESET NOD32** *Источник:* https://ru.wikipedia.org/wiki/ESET_NOD32?oldid=75458331 *Авторы:* Bubuka, YurikBot, Kurochka, APTEM, Roxis, GolerGkA, MaxSem, Lite, Vasiliy Faronov, Vlad2000Plus, The Wrong Man, Talexx, BotCat, Alexei Kouprianov, Gosh, SkyBon, Dgilmour, Bss, IwanS, BLISTHRV, JAnDbot, PBot, Gdn, Grenadine, HungerGhost, RoboMaxCyberSem, CommonsDelinker,

DonRumata, TanatOS, Rei-bot, Nick F0x, VasilievVV, Deerhunter, Aibot, Константин Б., Elmor, Holop, Alex.ryazantsev, Sorx00, UncleMartin, Loveless, Doca, Viplux, Alexanderwdark, Iakov, GrigorevMN, Rubin16, Павел ПМ, OKBot, Alexbot, Kinka, Andrey Albitov, Sans-etre, Goblin01, РобоСтася, Knowledge~ruwiki, Laim, Kvorum, AS, Muro Bot, AnatoliyTkachev, Iluvatar, AVB, Dimonich1, Ptbotgourou, Tumkir, Bootkiller, Mark Ekimov, Sergius1989, Yura93, VOVANBFG, Obersachsebot, ArthurBot, Vasyatka1, Ваан, Ludvig14, Xqbot, Tutaishy, Boodjoom85, Partyzan XXI, Artem Samarin, Valdis72, EmausBot, Drakosh, Web93onv, Impperial, Olezha 85, Википравитель, HRoestBot, Ареопагит, EugenG, Игорь Темиров, Dendesha, Wikifido, LordRimmon, Cinemantique, CAT Server, Zorgy131, Dima145, Lesless, CrazyBird~ruwiki, Rubinbot III, KPu3uC B Poccuu, Programman, Bierce, Alexej67, Addbot, Vladislav Chernyy, Dimon4ezzz, Apacersis, Programer47, Alena Mark и Аноним: 152

- **F-PROT Antivirus** *Источник:* https://ru.wikipedia.org/wiki/F-PROT_Antivirus?oldid=60854038 *Авторы:* PBot, WXP, Luckas-bot, EmausBot, LankLinkBot и Аноним: 1
- **F-Secure Anti-Virus** *Источник:* https://ru.wikipedia.org/wiki/F-Secure_Anti-Virus?oldid=63157890 *Авторы:* PBot, WXP, Lopatoid, Luckas-bot, EmausBot, LankLinkBot, H2Bot, Apacersis и Аноним: 6
- **G-DATA** *Источник:* https://ru.wikipedia.org/wiki/G-DATA?oldid=58539150 *Авторы:* Softy, VolkovBot, Fnaq, Ufim, AVB, Luckas-bot, Rubinbot, Obersachsebot, Xqbot, LucienBOT, Ботильда, TenBaseT, Vort, TobeBot, Small Bug, Anastasia86, Alex demin, WikitanvirBot, Wanderer Light, Vadim68 ferenets, Addbot и Аноним: 15
- **Graugon Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Graugon_Antivirus?oldid=68485450 *Авторы:* Nzeemin, Askarmuk, CheloVechek, Rtnick, MrFedikable, Tentatum и Аноним: 2
- **ICSA Labs** *Источник:* https://ru.wikipedia.org/wiki/ICSA_Labs?oldid=64075911 *Авторы:* Fuseau, Movses, Gdn, Analyzer (KODEP), РобоСтася, Obersachsebot, Sust, D'ohBot, MotnahpBot, Gipoza и Addbot
- **IKARUS Security Software** *Источник:* https://ru.wikipedia.org/wiki/IKARUS_Security_Software?oldid=60993852 *Авторы:* Askarmuk, PBot, RedAndr, Yaroslav Blanter, Alexanderwdark, Aquantrum, Четыре тильды, РобоСтася, AVB, Hairovich, Kaban2009, AntonST, Small Bug, ArchoNotron, EmausBot, LankLinkBot, RotlinkBot, Addbot и Аноним: 8
- **Kaspersky Mobile Security** *Источник:* https://ru.wikipedia.org/wiki/Kaspersky_Mobile_Security?oldid=71288479 *Авторы:* Sasha Krotov, Ghirlandajo, Putnik, BLISTHRV, PBot, WXP, Анатолич1, DILIN, Artemka373, Евгений Малинин, Rubinbot, ArthurBot, Qweedsa, DenisKrivosheev, Aglu, Partyzan XXI, Vort, ZéroBot, Викимонетчик, GODofAtoms, Addbot, Facenapalm и Аноним: 9
- **Malwarebytes' Anti-Malware** *Источник:* https://ru.wikipedia.org/wiki/Malwarebytes'{}_Anti-Malware?oldid=67849062 *Авторы:* Abarmot, Dipsy, PBot, VolkovBot, Skazi, Forajump, MystBot, Luckas-bot, Xqbot, U-bot, Ghuron, Хитрый гнУс, Zarkon-X, EmausBot, Википравитель, ChuispastonBot, Movses-bot, KrBot, WebCite Archiver, MerlIwBot, Patrias, Inlifeuser, FameownerBot и Аноним: 21
- **Microsoft Anti-Virus for Windows** *Источник:* https://ru.wikipedia.org/wiki/Microsoft_Anti-Virus_for_Windows?oldid=64304670 *Авторы:* Sealle и HumanEditorGames
- **Microsoft Security Essentials** *Источник:* https://ru.wikipedia.org/wiki/Microsoft_Security_Essentials?oldid=74549443 *Авторы:* IgorMagic, APTEM, OckhamTheFox, Teufel, Escarbot, Atorero, Carn, Dima1, Thijs!bot, BLISTHRV, JAnDbot, PBot, CommonsDelinker, Drozd, VolkovBot, Fnaq, Zimak, Askusnov, TXiKiBoT, Sonik, ShinePhantom, SieBot, Agent001, G0rn, Fx-man, Koliz, Alexbot, Zorrobot, Infernus, Muro Bot, K4dima, LaaknorBot, Amirobot, MystBot, Luckas-bot, SF007, Tumkir, Rubinbot, Lazyhawk, JackieBot, Doomsday nxt, Abigor, Xqbot, S0me1, Alexandr Pomorcev, Stoodiakv1, IMateo, D'ohBot, Khmm, S Snake, MondalorBot, Ботильда, Prowdtobegeek, Krassotkin, Softwayer, VanDerMelk, Evilutioner, Wform, Поцак, E7en, Taaraora, EmausBot, Drakosh, Лишь человек, Konjernb, D0wN b0i, GrouchoBot, ZéroBot, MrFedikable, Tar-Mairon, Altaviro, Ytopa, Odlan, Dadarik, Игорь Темиров, WikitanvirBot, LordRimmon, Movses-bot, Sergey 4, Exxxxxcel~ruwiki, WebCite Archiver, Dima145, Новосёлов Михаил, SpaceRu, MerlIwBot, MBHbot, Sealle, Well-Informed Optimist, Kojy, Дмитрий Ив. Самойлов, MrLambdaMu, Alexxsun, Папа рядом!, Po4teda, Блокнот, Itshaman, Addbot, Dimon4ezzz, KoroLion, Hoverage и Аноним: 112
- **NANO Антивирус** *Источник:* https://ru.wikipedia.org/wiki/NANO_%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81?oldid=75140422 *Авторы:* Vlad2000Plus, PBot, CommonsDelinker, Важнов Алексей Геннадьевич, Rlu, Dmitry Rozhkov, Bilderling, NoGo, U-bot, Sigwald, Nano.antivirus, †, Википравитель, Panchomoscow, ‡, KrBot, WebCite Archiver, Miss.hunter, Папа рядом!, Apacersis, Facenapalm, !болит и Аноним: 37
- **Norton AntiVirus** *Источник:* https://ru.wikipedia.org/wiki/Norton_AntiVirus?oldid=72391489 *Авторы:* Nikiforov, Snch, Roxis, Alex Kassarin, Alexei Kouprianov, Пиотровский Юрий, Escarbot, Bss, ZsergheiBot, BLISTHRV, PBot, Gdn, Rei-bot, TXiKiBoT, VVVBot-temp, SieBot, Peni, Loveless, WikiCle, BotMultichill, AlleborgoBot, Alexanderwdark, PixelBot, Alexbot, AlanNova, UR3IRS, MelancholieBot, AnatoliyTkachev, AVB, Luckas-bot, Animist, Ssorov, Misi91, Xqbot, Udmulu, Sigwald, WindBot, VAP+VYK, EmausBot, Википравитель, LASDORF, LankLinkBot, Александр Русский, Madam adamenko, KrBot, Ltanner2, FaustGT, Katty2110, Addbot, Apacersis, MarchHare1977 и Аноним: 22
- **Outpost Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Outpost_Antivirus?oldid=71740216 *Авторы:* APTEM, BLISTHRV, PBot, Peni, G0rn, Kinka, AVB, JLeks, EmausBot, HAL9000, LankLinkBot, Игорь Темиров, Kdm, Папа рядом!, Apacersis, BookBoy77 и Аноним: 8
- **Panda Security** *Источник:* https://ru.wikipedia.org/wiki/Panda_Security?oldid=70594164 *Авторы:* Escarbot, Thijs!bot, BLISTHRV, VolkovBot, ButkoBot, Zorrobot, Luckas-bot, Futball80, Rubinbot, Xqbot, MastiBot, WindBot, AntonST, Щербина, Ботильда, Алмаз92, Wikipandarus, ArchoNotron, Ripchip Bot, EmausBot, Animal-wiki, LankLinkBot, ChuispastonBot, Deniska47, Karachun, Alexxsun, Addbot и Аноним: 7
- **Qihoo 360 Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Qihoo_360_Antivirus?oldid=75378089 *Авторы:* Avmaksimov, CommonsDelinker, CheloVechek, Rubinbot, ДжеК87, KrBot, Mrkhlopov, Lucas Franke, WalkDark и Аноним: 17
- **Rising Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Rising_Antivirus?oldid=73517703 *Авторы:* Иван Тайга, VolkovBot, CheloVechek, SieBot, AmphBot, EmausBot, EleferenBot, Addbot, Tentatum и Аноним: 8
- **SafenSoft SysWatch** *Источник:* https://ru.wikipedia.org/wiki/SafenSoft_SysWatch?oldid=65403420 *Авторы:* Bezik, PBot, Ivan A. Krestinin, U-bot, Rashevskiy, Tar-Mairon, KrBot, WebCite Archiver и Аноним: 2
- **TrustPort a.s.** *Источник:* https://ru.wikipedia.org/wiki/TrustPort_a.s.?oldid=72295905 *Авторы:* Alex Smotrov, VolkovBot, Jackie, РобоСтася, MystBot, Luckas-bot, Rubinbot, Ivan A. Krestinin, Gizzatullin, EmausBot, Роман Курносенко, H2Bot, WikitanvirBot, Movses-bot, KrBot, Ambu, Jicarilla, Volkov V, Facenapalm, Tentatum и Аноним: 7

- **TrustPort Antivirus** *Источник:* https://ru.wikipedia.org/wiki/TrustPort_Antivirus?oldid=60854907 *Авторы:* Infovarius, PBot, РобоСтася, Rubinbot, Ivan A. Krestinin, ArtTrapeza, KrBot, Ambu, Volkov V, Apacersis и Аноним: 6
- **TrustPort Security Elements** *Источник:* https://ru.wikipedia.org/wiki/TrustPort_Security_Elements?oldid=56129117 *Авторы:* Rubinbot, Ivan A. Krestinin, KrBot, Ambu и Аноним: 1
- **USB Disk Security** *Источник:* https://ru.wikipedia.org/wiki/USB_Disk_Security?oldid=68587665 *Авторы:* PBot, Akim Dubrow, Mansur321, Википравитель, WebCite Archiver и Аноним: 3
- **VirusTotal** *Источник:* https://ru.wikipedia.org/wiki/VirusTotal?oldid=74550545 *Авторы:* Hayk, Egor, Cheops, A5b, Fanny, VolkovBot, TXiKiBoT, TarzanASG, Alex.ryazantsev, Divega, AlanNova, РобоСтася, Luckas-bot, Ptbotgourou, Rubinbot, Yura93, Obersachsebot, Rivertime, Leo Tomcat, Okras, VadimIppolitov, Greggh, Xqbot, LucienBOT, Tnktnp, Partyzan XXI, Armenian Baron, Vort, TobeBot, Exion~ruwiki, EmausBot, ???4, Діоген Ангел, ZéroBot, Centurion198, Marcus Qwertyus, Ntfs.hard, WikitanvirBot, Abc41, WebCite Archiver, Well-Informed Optimist, Miss.hunter, Dart Raiden, Папа рядом!, Addbot, Zloi 4el, Max cron, Alex NB IT и Аноним: 38
- **Windows Live OneCare** *Источник:* https://ru.wikipedia.org/wiki/Windows_Live_OneCare?oldid=74549694 *Авторы:* Butko, Sasha Krotov, BotCat, User№101, VolkovBot, Victoria, ButkoBot, Holop, X-Pilot, VVVBot, Dzmuh, Ptbotgourou, Fanni 93, Okras, Xqbot, Sigwald, Tpyvvikky, Krassotkin, SpaceRu, Addbot, Dimon4ezzz, Avbiolog и Аноним: 9
- **Zillya!** *Источник:* https://ru.wikipedia.org/wiki/Zillya!?oldid=74511166 *Авторы:* Snch, Butko, Insider, Dima1, BLISTHRV, PBot, Vicpeters, Nickispeaki, VolkovBot, Anodonta, Cantor, Bilderling, Leszek Jańczuk, Pieter Baas, Luch4, D.bratchuk, Cult of rina, U-bot, Structor, Atlas86, Partyzan XXI, Urotsukidoji, Artem Samarin, Pavel55, Drakosh, ReckouNT, KrBot, MarShaLL22, Well-Informed Optimist, Addbot, Falcon256, MarchHare1977, Tentatum, Manblackpen и Аноним: 13
- **Антивирус Касперского** *Источник:* https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81_%D0%9A%D0%B0%D1%81%D0%BF%D0%B5%D1%80%D1%81%D0%BA%D0%BE%D0%B3%D0%BE?oldid=75258139 *Авторы:* Wind, Torin, Александр Мотин, APTEM, A5b, Sasha Krotov, Nikolay Nikolaevich Fedotov, Putnik, BLISTHRV, PBot, Gdn, Alex Smotrov, VolkovBot, Aleksandrit, Vs64vs, Holop, SieBot, Alex.ryazantsev, Peni, Alexanderwdark, Iakov, GrigorevMN, Botinko, Jeka3000, Kinka, Different.local, РобоСтася, Kvorum, Erud, AVB, Евгений Малинин, Luckas-bot, Tumkir, Dencher, Obersachsebot, Fanni 93, Xqbot, WindBot, Aglu, Partyzan XXI, Щербина, Kav7, RedBot, Prowdtobegeek, Convallaria majalis, Duchesse~ruwiki, BOOMER 74, EmausBot, GrouchoBot, ZéroBot, Википравитель, Georgij-pyankov, Centurion198, LankLinkBot, OneLittleMouse, Oleg Yunakov, Wikifido, LordRimmon, KrBot, WebCite Archiver, MarShaLL22, FaustGT, MBHbot, Programman, К.Артём.1, Trava152, Vitalkad, Prizvel, Наумов Андрей, Alexxsun, Andiorahn, Addbot, RWBYRubyRose и Аноним: 97
- **ВирусБлокАда** *Источник:* https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%83%D1%81%D0%91%D0%BB%D0%BE%D0%BA%D0%90%D0%B4%D0%B0?oldid=73161699 *Авторы:* Bezik, Unomano, Putnik, BLISTHRV, PBot, Dreamer.mas, Flrn, Деев Алексей, Bilderling, LatitudeBot, Lazyhawk, Esssenin, D'ohBot, Tretyak, Gemorroj, Win32neshto, Dima Le, Movses-bot, Karachun, Magnus-vvvv, Robiteria, Virusblokada, Addbot, Deamhan91 и Аноним: 21
- **Лжеантивирус** *Источник:* https://ru.wikipedia.org/wiki/%D0%9B%D0%B6%D0%B5%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81?oldid=74685081 *Авторы:* Mercury, AVRS, Askusnov, Elmor, Rubinbot, Dmbaturin, EmausBot, Arbnos, Drakosh, Википравитель, H2Bot, Byzantine, WebCite Archiver, MerlIwBot, Saint Johann, User7777, Луговкин, NSauk, RotlinkBot, Whydoesitfeelsogood и Аноним: 14
- **Ревизор (программа)** *Источник:* https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B2%D0%B8%D0%B7%D0%BE%D1%80_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0)?oldid=70938881 *Авторы:* Shade, Ufim, РобоСтася, Tretyak, Partyzan XXI, Valdis72, KrBot, Gipoza, Наумов Андрей, Луговкин и Аноним: 6
- **Резидентная защита** *Источник:* https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B7%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0?oldid=21458354 *Авторы:* Halyavin, С. Л., Cheops, MaxSem, IwanS, Berserkerus, Peni, Laim и Аноним: 3
- **Clam Antivirus** *Источник:* https://ru.wikipedia.org/wiki/Clam_Antivirus?oldid=74870778 *Авторы:* YurikBot, Roxis, Csman, MaxSem, Vlad2000Plus, Sergei, Никольский Ярослав, ZsergheiBot, Thijs!bot, BLISTHRV, Quadro, PBot, Gdn, AVRS, Alex Smotrov, VolkovBot, One half 3544, Idioma-bot, Plazzmex, ButkoBot, Be nt all, TXiKiBoT, Holop, X-Pilot, Synthebot, SieBot, Alex.ryazantsev, Loveless, Analyzer (KODEP), Montrezor, CarsracBot, Jsg08, AnatoliyTkachev, AVB, SF007, Ptbotgourou, Yodal, Rubinbot, Obersachsebot, Izomorti, AlexeyChupahin, Xqbot, Anton I. Steklov, DenisKrivosheev, EmausBot, Kirill Mingulov, Станислав Митичкин, Deepak-nsk, AbiyoyoBot, WikitanvirBot, KrBot, Sashakrasnoyarsk, MBHbot, HeimerDrey, Makecat-bot, YFdyh-bot, Martin Devil, Mrkhlopov, Addbot, Citing Bot, Olzirg и Аноним: 28
- **ClamWin** *Источник:* https://ru.wikipedia.org/wiki/ClamWin?oldid=72264383 *Авторы:* YurikBot, Roxis, Csman, Evilbot, MaxSem, DmitrySorokin, Grey horse, Sergei, Nbr, Edwardspec TalkBot, RuED, ZsergheiBot, Thijs!bot, BLISTHRV, PBot, Gdn, VolkovBot, DodekBot~ruwiki, Plazzmex, Holop, SieBot, GrigorevMN, DragonBot, Макеенков Сергей, Alecs.bot, Ginosbot, AnatoliyTkachev, AVB, SF007, Ptbotgourou, Bootkiller, Insuranze, Xqbot, Structor, Amychok, Mutari-Dirk, Deepak-nsk, Sasa13e, LankLinkBot, KrBot, Azag-Thoth, MBHbot, Patrias, Addbot, Glovacki, Citing Bot и Аноним: 24
- **WinPooch** *Источник:* https://ru.wikipedia.org/wiki/WinPooch?oldid=60841494 *Авторы:* Cheops, BLISTHRV, PBot, Gdn, VolkovBot, ButkoBot, Be nt all, AVB, Luckas-bot, AbiyoyoBot, MerlIwBot, Addbot и Аноним: 6

100.3.2. Изображения

- **Файл:AVG_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/3/39/AVG_logo.png *Лицензия:* Добросовестное использование *Авторы:* http://www.avg.com/ca-en/images *Художник:* AVG
- **Файл:AVG_wordmark.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/6b/AVG_wordmark.png *Лицензия:* Public domain *Авторы:* http://aa-download.avg.com/filedir/promo/press/press_logo_avg.png *Художник:* AVG Technologies
- **Файл:AVZ_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/0d/AVZ_logo.png *Лицензия:* Добросовестное использование *Авторы:* AVZ *Художник:* Олег Зайцев
- **Файл:Acronis_antivirus_2010.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/f7/Acronis_antivirus_2010.png *Лицензия:* Добросовестное использование *Авторы:* сделан на компьютере участник:WXP *Художник:* Acronis Inc.

- **Файл:Acronis_antivirus_exp.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/0a/Acronis_antivirus_exp.png *Лицензия:* Добросовестное использование *Авторы:* сделан на компьютере участник:WXP *Художник:* Acronis Inc.
- **Файл:Acronis_antivirus_nov.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/3/32/Acronis_antivirus_nov.png *Лицензия:* Добросовестное использование *Авторы:* сделан на компьютере участник:WXP *Художник:* Acronis Inc.
- **Файл:Activevirusshield.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/0e/Activevirusshield.png *Лицензия:* Добросовестное использование *Авторы:* Программа *Художник:* Лаборатория Касперского, AOL
- **Файл:Advanced_SystemCare.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/4/4b/Advanced_SystemCare.png *Лицензия:* Добросовестное использование *Авторы:* http://ru.iobit.com/wp-content/themes/iobit/img/ascpro00.png *Художник:* IObit
- **Файл:Advanced_SystemCare_Ultimate.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/2/24/Advanced_SystemCare_Ultimate.png *Лицензия:* Добросовестное использование *Авторы:* http://ru.iobit.com/wp-content/themes/iobit/img/asc_u000.png *Художник:* IObit
- **Файл:Agnitum_outpost_Antivirus.PNG** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/04/Agnitum_outpost_Antivirus.PNG *Лицензия:* Добросовестное использование *Авторы:* www.agnitum.ru *Художник:* Agnitum
- **Файл:Aidstest.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/b/b0/Aidstest.png *Лицензия:* Добросовестное использование *Авторы:* скриншот результата работы программы *Художник:* автор: Лозинский Дмитрий Николаевич, правообладатель: ЗАО "ДиалогНаука"
- **Файл:Ambox_PR.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/b/b3/Ambox_PR.svg *Лицензия:* Public domain *Авторы:* self-made in Adobe Illustrator and Inkscape *Художник:* penubag
- **Файл:Ambox_outdated_serious.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/8/8f/Ambox_outdated_serious.svg *Лицензия:* Public domain *Авторы:* собственная работа *Художник:* penubag, Tkgd2007 made the clock
- **Файл:Ambox_scales.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/5/5c/Ambox_scales.svg *Лицензия:* Public domain *Авторы:* self-made using inkscape and based off of Image:Emblem-scales.svg *Художник:* penubag and Tkgd2007 (scales image)
- **Файл:Ashampoo_AntiSpyWare.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/1/10/Ashampoo_AntiSpyWare.png *Лицензия:* Добросовестное использование *Авторы:* http://img.ashampoo.com/ashampoo.com_images/img/1/products/0149/en/screenshots/scr_0149_en.jpg *Художник:* Ashampoo
- **Файл:Ashampoo_AntiVirus.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/5/51/Ashampoo_AntiVirus.png *Лицензия:* Добросовестное использование *Авторы:* http://img.ashampoo.com/ashampoo.com_images/img/1/products/0045/en/screenshots/0045_scr_en_large.png *Художник:* Ashampoo
- **Файл:Ashampoo_Firewall.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/04/Ashampoo_Firewall.jpg *Лицензия:* Добросовестное использование *Авторы:* http://img.ashampoo.com/ashampoo.com_images/img/1/products/0050/uk/screenshots/0050_scr_en_large.jpg *Художник:* Ashampoo
- **Файл:Avast.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/f6/Avast.png *Лицензия:* Добросовестное использование *Авторы:* Программа *Художник:* AVAST Software
- **Файл:Avast_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/b/be/Avast_logo.png *Лицензия:* Добросовестное использование *Авторы:* http://www.avast.com/ *Художник:* AVAST Software
- **Файл:Avira_Antivir_FREE.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/f8/Avira_Antivir_FREE.png *Лицензия:* Добросовестное использование *Авторы:* Программа Avira AntiVir *Художник:* Avira GmbH
- **Файл:Avira_logo_2011.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/94/Avira_logo_2011.png *Лицензия:* Public domain *Авторы:* www.avira.com *Художник:* Avira Operations GmbH & Co. KG
- **Файл:Avz4.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/b/b4/Avz4.jpg *Лицензия:* Добросовестное использование *Авторы:* скриншот снят на рабочем ПК пользователя Участник:Gdn *Художник:* Олег Зайцев
- **Файл:BWMeterScreenshot.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/f7/BWMeterScreenshot.png *Лицензия:* Добросовестное использование *Авторы:* http://www.desksoft.com/BWMeter/bmscreenshot_large.png *Художник:* DeskSoft
- **Файл:Bitdefender_dragon_wolf.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/2/23/Bitdefender_dragon_wolf.png *Лицензия:* Copyrighted free use *Авторы:*
- Source web page: bitdefenderantiviruscoupon.com *Художник:* BitDefender
- **Файл:Broom_icon.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/2/2c/Broom_icon.svg *Лицензия:* GPL *Авторы:* http://www.kde-look.org/content/show.php?content=29699 *Художник:* gg3po (Tony Tony), SVG version by User:Booyabazooka
- **Файл:Bullguard_Intenet_Security.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/4/48/Bullguard_Intenet_Security.png *Лицензия:* Добросовестное использование *Авторы:* сделан на компьютере участник:WXP *Художник:* BullGuard Ltd.
- **Файл:Bus_icon.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/c/ca/Bus_icon.svg *Лицензия:* Public domain *Авторы:* No machine-readable source provided. Own work assumed (based on copyright claims). *Художник:* Сведения об авторе отсутствуют или не читаются программно. Предположительно Booyabazooka (основываясь на заявлении об авторском праве).
- **Файл:ClamAV.jpeg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/b/b8/ClamAV.jpeg *Лицензия:* CC-BY-SA-3.0 *Авторы:* http://www.clamav.net/ *Художник:* Equipo ClamAV
ClamAV is a registered trademark of Cisco Systems Inc.
- **Файл:ClamWin_Logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/94/ClamWin_Logo.png *Лицензия:* GPL *Авторы:* Original image uploaded by w:User:PatrickPatience. *Художник:* © ClamWin Free Antivirus
ClamWin™ is a trademark of ClamWin Pty Ltd.
- **Файл:ClamWin_on_Ubuntu.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/d/db/ClamWin_on_Ubuntu.png *Лицензия:* GPL *Авторы:* http://hacktolive.org/images *Художник:* http://hacktolive.org
- **Файл:Clam_Tk_Virus_Scanner.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/6c/Clam_Tk_Virus_Scanner.png *Лицензия:* GPL *Авторы:* ? *Художник:* ?

- **Файл:Comdo_Firewall.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/c5/Comdo_Firewall.png *Лицензия:* Добросовестное использование *Авторы:* Comodo Internet Security *Художник:* Comodo Group
- **Файл:Commons-logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/4/4a/Commons-logo.svg *Лицензия:* Public domain *Авторы:* This version created by Pumbaa, using a proper partial circle and SVG geometry features. (Former versions used to be slightly warped.) *Художник:* SVG version was created by User:Grunt and cleaned up by 3247, based on the earlier PNG version, created by Reidab.
- **Файл:Comodo_Internet_Security_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/1/16/Comodo_Internet_Security_logo.png *Лицензия:* Добросовестное использование *Авторы:* Comodo Internet Security *Художник:* Comodo Group
- **Файл:EICAR.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/0/08/EICAR.png *Лицензия:* CC BY-SA 4.0 *Авторы:* собственная работа *Художник:* LillySmithers
- **Файл:ESET_antivir_7_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/63/ESET_antivir_7_logo.png *Лицензия:* Public domain *Авторы:* ESET spol s.r.o. *Художник:* ESET spol s.r.o.
- **Файл:Emblem-important.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/4/4c/Emblem-important.svg *Лицензия:* Public domain *Авторы:* The Tango! Desktop Project *Художник:* The people from the Tango! project
- **Файл:F-Prot_Antivirus.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/c1/F-Prot_Antivirus.png *Лицензия:* Добросовестное использование *Авторы:* скриншот сделан на компьютере участник:WXP *Художник:* FRISK Software Int.
- **Файл:F-secure_antivirus_gadget.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/c1/F-secure_antivirus_gadget.png *Лицензия:* Добросовестное использование *Авторы:* сделан на компьютере участник:WXP *Художник:* F-Secure Corp.
- **Файл:F-secure_antivirus_mw.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/5/5c/F-secure_antivirus_mw.png *Лицензия:* Добросовестное использование *Авторы:* сделан на компьютере участник:WXP *Художник:* F-Secure Corp.
- **Файл:Firewall.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png *Лицензия:* CC BY-SA 3.0 *Авторы:* Feito por mim *Художник:* Bruno Pedrozo
- **Файл:Firewall_bw.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/1/10/Firewall_bw.png *Лицензия:* GPL *Авторы:* http://www.opendesktop.org/content/show.php?content=72618 *Художник:* DBGthekafu
- **Файл:Flag_of_Germany.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/b/ba/Flag_of_Germany.svg *Лицензия:* Public domain *Авторы:* ? *Художник:* ?
- **Файл:Flag_of_Israel.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/d/d4/Flag_of_Israel.svg *Лицензия:* Public domain *Авторы:* http://www.mfa.gov.il/MFA/History/Modern%20History/Israel%20at%2050/The%20Flag%20and%20the%20Emblem *Художник:* "The Provisional Council of State Proclamation of the Flag of the State of Israel" of 25 Tishrei 5709 (28 October 1948) provides the official specification for the design of the Israeli flag.
- **Файл:Flag_of_Romania.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/7/73/Flag_of_Romania.svg *Лицензия:* Public domain *Авторы:* собственная работа *Художник:* AdiJapan
- **Файл:Flag_of_Russia.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/f/f3/Flag_of_Russia.svg *Лицензия:* Public domain *Авторы:* Государственный флаг Российской Федерации. Цвета флага: (Blue - Pantone 286 C, Red - Pantone 485 C) взяты из [1][2][3][4] *Художник:* Zscout370
- **Файл:Flag_of_Spain.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/9a/Flag_of_Spain.svg *Лицензия:* CC0 *Авторы:* ["Sodipodi.com Clipart Gallery". Original link no longer available] *Художник:* Pedro A. Gracia Fajardo, escudo de Manual de Imagen Institucional de la Administración General del Estado
- **Файл:Flag_of_the_People's_Republic_of_China.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Flag_of_the_People%27s_Republic_of_China.svg *Лицензия:* Public domain *Авторы:* собственная работа, http://www.protocol.gov.hk/flags/eng/n_flag/design.html *Художник:* Drawn by User:SKopp, redrawn by User:Denelson83 and User:Zscout370
- **Файл:Flag_of_the_United_States.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/a/a4/Flag_of_the_United_States.svg *Лицензия:* Public domain *Авторы:* SVG implementation of U. S. Code: Title 4, Chapter 1, Section 1 [1] (the United States Federal "Flag Law"). *Художник:* Dbenbenn, Zscout370, Jacobolus, Indolences, Technion.
- **Файл:Folder_Hexagonal_Icon.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/4/48/Folder_Hexagonal_Icon.svg *Лицензия:* CC-BY-SA-3.0 *Авторы:* Собственная работа на основе: Folder.gif. *Художник:* **Оригинал:** John Cross **Векторизация:** Shazz
- **Файл:FortiGate-100D.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/2/25/FortiGate-100D.jpg *Лицензия:* CC BY-SA 2.5 *Авторы:* fortinet.com *Художник:* fortinet
- **Файл:Fortinet_Logo.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/62/Fortinet_Logo.jpg *Лицензия:* Public domain *Авторы:* fortinet.com *Художник:* Fortinet
- **Файл:GDATA.svg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/0b/GDATA.svg *Лицензия:* Добросовестное использование *Авторы:* http://www.gdata.de/ *Художник:* G DATA Software AG
- **Файл:Gufw_10.04.4.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/b/ba/Gufw_10.04.4.png *Лицензия:* GPL *Авторы:* http://gufw.tuxfamily.org *Художник:* ?
- **Файл:Heckert_GNU_white.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/2/22/Heckert_GNU_white.svg *Лицензия:* CC BY-SA 2.0 *Авторы:* gnu.org *Художник:* Aurelio A. Heckert <aurium@gmail.com>
- **Файл:IKARUS_Security_Software_Ges.m.b.H._logo_.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/c1/IKARUS_Security_Software_Ges.m.b.H._logo_.jpg *Лицензия:* Добросовестное использование *Авторы:* MURAVA — дистрибутор IKARUS Security Software Ges.m.b.H. в РФ *Художник:* IKARUS Security Software GmbH
- **Файл:IPFire_Logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/b/b1/IPFire_Logo.png *Лицензия:* Public domain *Авторы:* Artist *Художник:* Halit YEŞİL
- **Файл:Icsalabs_logo.gif** *Источник:* https://upload.wikimedia.org/wikipedia/ru/1/17/Icsalabs_logo.gif *Лицензия:* Добросовестное использование *Авторы:* http://www.icsalabs.com/ *Художник:* ICSA

- **Файл:Iptables-traversal.svg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/f4/Iptables-traversal.svg *Лицензия:* CC BY-SA 3.0 *Авторы:* http://antono.info/files/images/iptables-traverse.svg *Художник:* Antono Vasiljev <antono.vasiljev@gmail.com>
- **Файл:Iptablesfb.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/1/11/Iptablesfb.png *Лицензия:* GPL *Авторы:* By nnz1024 *Художник:* Netfilter Core Team
- **Файл:JeticoLogo.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/e/e1/JeticoLogo.jpg *Лицензия:* Добросовестное использование *Авторы:* www.jetico.com *Художник:* Jetico Corporation
- **Файл:KAV_KIS_Logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/6/66/KAV_KIS_Logo.svg *Лицензия:* Добросовестное использование *Авторы:* Исполняемый файл (avp.exe) *Художник:* Лаборатория Касперского
- **Файл:KasperskyAntiVirus2012.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/fc/KasperskyAntiVirus2012.png *Лицензия:* Добросовестное использование *Авторы:* kaspersky.ru *Художник:* ЗАО "Лаборатория Касперского"
- **Файл:KasperskyInternetSecurity2012.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/a/a1/KasperskyInternetSecurity2012.png *Лицензия:* Добросовестное использование *Авторы:* kaspersky.ru *Художник:* ЗАО "Лаборатория Касперского"
- **Файл:Kms9_box_ru.tif** *Источник:* https://upload.wikimedia.org/wikipedia/ru/9/97/Kms9_box_ru.tif *Лицензия:* Добросовестное использование *Авторы:* Официальный сайт *Художник:* Лаборатория Касперского
- **Файл:Kms9main.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/01/Kms9main.png *Лицензия:* Добросовестное использование *Авторы:* Официальный сайт *Художник:* Лаборатория Касперского
- **Файл:MSAV.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/0/09/MSAV.png *Лицензия:* Добросовестное использование *Авторы:* en:File:MSAV.png *Художник:* Microsoft
- **Файл:MSE_Threat_Alert.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/4/41/MSE_Threat_Alert.png *Лицензия:* Добросовестное использование *Авторы:* Английский раздел Википедии *Художник:* Microsoft
- **Файл:M_box.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/94/M_box.svg *Лицензия:* Public domain *Авторы:* Собственная работа на основе: File:Microsoft.svg *Художник:* Ariesk47 (talk)
- **Файл:Malwarebytes_logo_and_wordmark.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/2/2a/Malwarebytes_logo_and_wordmark.png *Лицензия:* Public domain *Авторы:* https://www.malwarebytes.org/partners/resources/ *Художник:* Изначально этот файл был загружен участником JC713 из английский Википедия
- **Файл:Merge-split-transwiki_default.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/e/e0/Merge-split-transwiki_default.svg *Лицензия:* Public domain *Авторы:* Self-made, based on by Father Goose. Arrows derived from . *Художник:* Davidgothberg
- **Файл:Microsoft_Security_Essentials.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/9/90/Microsoft_Security_Essentials.png *Лицензия:* Добросовестное использование *Авторы:* en:File:Microsoft Security Essentials.png *Художник:* Microsoft
- **Файл:Microsoft_Security_Essentials_Genuine_Notification.PNG** *Источник:* https://upload.wikimedia.org/wikipedia/ru/9/95/Microsoft_Security_Essentials_Genuine_Notification.PNG *Лицензия:* Добросовестное использование *Авторы:* en:file:Microsoft Security Essentials Genuine Notification.PNG *Художник:* Microsoft
- **Файл:Microsoft_Security_Essentials_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/f8/Microsoft_Security_Essentials_logo.png *Лицензия:* Добросовестное использование *Авторы:* http://en.wikipedia.org/wiki/File:Microsoft_Security_Essentials_logo.png *Художник:* Microsoft
- **Файл:Monitor_padlock.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/7/73/Monitor_padlock.svg *Лицензия:* CC BY-SA 3.0 *Авторы:* Transferred from en.wikipedia; transferred to Commons by User:Logan using CommonsHelper. *Художник:* Lunarbunny (talk). Original uploader was Lunarbunny at en.wikipedia
- **Файл:NANO_AntiVirus_screenshot.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/5/5e/NANO_AntiVirus_screenshot.png *Лицензия:* Добросовестное использование *Авторы:* Собственная работа *Художник:* ООО «НАНО Секьюрити»
- **Файл:NANO_antivirus_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/a/a1/NANO_antivirus_logo.png *Лицензия:* Добросовестное использование *Авторы:* Собственная работа *Художник:* ООО «НАНО Секьюрити»
- **Файл:NISLogo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/a/af/NISLogo.png *Лицензия:* Добросовестное использование *Авторы:* Norton Internet Security *Художник:* Symantec
- **Файл:Netfilter-diagram-rus.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/a/ad/Netfilter-diagram-rus.png *Лицензия:* Общественное достояние *Авторы:* Собственная работа *Художник:* Участник:Tetromino
- **Файл:Netfilter-packet-flow.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/3/37/Netfilter-packet-flow.svg *Лицензия:* CC BY-SA 3.0 *Авторы:* собственная работа, Origin SVG PNG *Художник:* Jengelh
- **Файл:Nis2010mainscreen.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/6/6c/Nis2010mainscreen.jpg *Лицензия:* Добросовестное использование *Авторы:* Norton Internet Security *Художник:* Symantec
- **Файл:No_iwiki_template.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/4/45/No_iwiki_template.svg *Лицензия:* Public domain *Авторы:* Wikipedia-logo-v2-en.svg: *Художник:* Urutseg, Amit6, Юкатан, Ain92

- **Файл:Norton360v3.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/8/82/Norton360v3.png *Лицензия:* Добросовестное использование *Авторы:* Главное окно программы Norton 360 *Художник:* Symantec Corporation
- **Файл:Norton_360_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/fe/Norton_360_logo.png *Лицензия:* Добросовестное использование *Авторы:* Компания SYMANTEC *Художник:* Symantec
- **Файл:Norton_AntiVirus_Logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/c6/Norton_AntiVirus_Logo.svg *Лицензия:* Добросовестное использование *Авторы:* ru.norton.com *Художник:* Symantec Corporation
- **Файл:Norton_Antivirus.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/a/a8/Norton_Antivirus.png *Лицензия:* Добросовестное использование *Авторы:* http://www.antivirusware.com/norton-antivirus/screenshots/ *Художник:* Symantec Corporation
- **Файл:Norton_Internet_Security_2009.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/f9/Norton_Internet_Security_2009.png *Лицензия:* Добросовестное использование *Авторы:* Symantec *Художник:* Symantec
- **Файл:Nuvola_apps_important_recycle.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/0/09/Nuvola_apps_important_recycle.svg *Лицензия:* LGPL *Авторы:* → → → → vectorized by uploader *Художник:* David Vignoni, Bastique, EvilHom3r, SolarUSA, Rocket000
- **Файл:Online_Armor_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/f/ff/Online_Armor_logo.png *Лицензия:* Добросовестное использование *Авторы:* http://rus.tallemu.com/downloads.html *Художник:* Tall Emu Pty Ltd.
- **Файл:Online_Armor_screenshot.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/ca/Online_Armor_screenshot.png *Лицензия:* Добросовестное использование *Авторы:* Online Armor Free *Художник:* Tall Emu Pty Ltd.
- **Файл:Outpost.gif** *Источник:* https://upload.wikimedia.org/wikipedia/ru/5/56/Outpost.gif *Лицензия:* Добросовестное использование *Авторы:* http://www.agnitum.ru/images/outpost/screens/outpost-7-5/001.png *Художник:* Agnitum Ltd.
- **Файл:PC_Tools_FW_plus.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/6/6f/PC_Tools_FW_plus.png *Лицензия:* Добросовестное использование *Авторы:* http://www.pctools.com/res/images/firewall/screenshot-ru.gif *Художник:* PC Tools
- **Файл:PC_Tools_FW_plus_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/7/7c/PC_Tools_FW_plus_logo.png *Лицензия:* Добросовестное использование *Авторы:* http://www.pctools.com/res/images/sd/title_fw.gif *Художник:* PC Tools
- **Файл:Panda-security-company-logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/e/eb/Panda-security-company-logo.png *Лицензия:* Добросовестное использование *Авторы:* http://www.pandasecurity.com/ *Художник:* Panda Security SL
- **Файл:Panda_Cloud_AV_Free.PNG** *Источник:* https://upload.wikimedia.org/wikipedia/ru/a/a1/Panda_Cloud_AV_Free.PNG *Лицензия:* Добросовестное использование *Авторы:* Panda Cloud AV 1.3 *Художник:* Panda Security
- **Файл:Panda_Cloud_Antivirus_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/b/b5/Panda_Cloud_Antivirus_logo.png *Лицензия:* Добросовестное использование *Авторы:* Panda Cloud Antivirus *Художник:* Panda Security SL
- **Файл:Personal_firewall.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/1/1f/Personal_firewall.svg *Лицензия:* CC BY 3.0 *Авторы:* selbst erstellt mithilfe von xfig und der xfig-libaries. *Художник:* Harald Mühlböck
- **Файл:Pfs-logo-vector.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/f/fb/Pfs-logo-vector.svg *Лицензия:* Copyrighted free use *Авторы:* self-made using potrace and Inkscape *Художник:* DanielSHaischt
- **Файл:Pfsense215.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/d/d4/Pfsense215.jpg *Лицензия:* CC BY-SA 4.0 *Авторы:* собственная работа *Художник:* Dkgnim
- **Файл:Planned_section.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/e/ec/Planned_section.svg *Лицензия:* CC BY-SA 3.0 *Авторы:*
- Blank_template.svg *Художник:* Blank_template.svg: Urutseg
- **Файл:Portal.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/c/c9/Portal.svg *Лицензия:* CC BY 2.5 *Авторы:*
  - Portal.svg

  Художник: Portal.svg: Pepetps
- **Файл:Question_book-2.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/d/d6/Question_book-2.svg *Лицензия:* CC-BY-SA-3.0 *Авторы:* en.wikipedia.org *Художник:* Originally designed by Equazcion (en:Image:Question book.png}.
- **Файл:Rising_Anti-Virus.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/0/09/Rising_Anti-Virus.jpg *Лицензия:* Public domain *Авторы:* собственная работа *Художник:* Иван Тайга

- **Файл:Rising_Logo.gif** *Источник:* https://upload.wikimedia.org/wikipedia/commons/7/7b/Rising_Logo.gif *Лицензия:* Public domain *Авторы:* собственная работа *Художник:* Иван Тайга
- **Файл:Rou000t666erx9.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/2/2f/Rou000t666erx9.jpg *Лицензия:* CC-BY-SA-3.0 *Авторы:* ? *Художник:* ?
- **Файл:Searchtool.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/61/Searchtool.svg *Лицензия:* LGPL *Авторы:* http://ftp.gnome.org/pub/GNOME/sources/gnome-themes-extras/0.9/gnome-themes-extras-0.9.0.tar.gz *Художник:* David Vignoni, Ysangkok
- **Файл:Shorewall_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/8/85/Shorewall_logo.png *Лицензия:* CC BY-SA 2.5 za *Авторы:* http://www.shorewall.net/shorewall_index.htm#Logo *Художник:* Gareth Davies of Thusa
- **Файл:Snslogo.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/1/11/Snslogo.png *Лицензия:* CC BY-SA 3.0 *Авторы:* www.safensoft.com *Художник:* SafenSoft Ltd.
- **Файл:Symbol_book_class2.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/8/89/Symbol_book_class2.svg *Лицензия:* CC BY-SA 2.5 *Авторы:* Mad by Lokal_Profil by combining: *Художник:* Lokal_Profil
- **Файл:Symbol_question.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/e/e0/Symbol_question.svg *Лицензия:* Public domain *Авторы:* ? *Художник:* ?
- **Файл:System-installer.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/d/db/System-installer.svg *Лицензия:* Public domain *Авторы:* The Tango! Desktop Project *Художник:* The people from the Tango! project
- **Файл:TI-logojpg.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/d/d9/TI-logojpg.jpg *Лицензия:* Public domain *Авторы:* собственная работа *Художник:* Смарт-Софт
- **Файл:TrustPort_logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/a/a9/TrustPort_logo.svg *Лицензия:* Public domain *Авторы:* Archives of TrustPort a.s. *Художник:* TrustPort a.s.
- **Файл:USBGuard-icon.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/4/41/USBGuard-icon.png *Лицензия:* Добросовестное использование *Авторы:* http://www.zbshareware.com/ *Художник:* Zbshareware Lab
- **Файл:USB_Disk_Security.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/b/bc/USB_Disk_Security.png *Лицензия:* Добросовестное использование *Авторы:* Программа *Художник:* Zbshareware Lab
- **Файл:UbuntuCoF.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/9e/UbuntuCoF.svg *Лицензия:* Public domain *Авторы:* Ubuntu Visual Identity *Художник:* Canonical Ltd
- **Файл:Ubuntu_logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/9d/Ubuntu_logo.svg *Лицензия:* Public domain *Авторы:* Ubuntu Visual Identity *Художник:* Canonical Ltd
- **Файл:VirusTotal-logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/a/a5/VirusTotal-logo.png *Лицензия:* Добросовестное использование *Авторы:* virustotal.com *Художник:* Hispasec Sistemas
- **Файл:Wikibooks-logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg *Лицензия:* CC BY-SA 3.0 *Авторы:* собственная работа *Художник:* User:Bastique, User:Ramac et al.
- **Файл:Wikitext-ru.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/4/47/Wikitext-ru.svg *Лицензия:* Public domain *Авторы:* made by Inkscape *Художник:* self
- **Файл:Windows_Firewall_Icon.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/d/d8/Windows_Firewall_Icon.png *Лицензия:* Добросовестное использование *Авторы:* Собственная работа *Художник:* Microsoft
- **Файл:Windows_Firewall_Vista.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/b/b7/Windows_Firewall_Vista.png *Лицензия:* Добросовестное использование *Авторы:* Windows Vista *Художник:* Microsoft
- **Файл:Windows_Firewall_XP_SP2.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/cc/Windows_Firewall_XP_SP2.png *Лицензия:* Добросовестное использование *Авторы:* Собственный скриншот *Художник:* Micrsoft
- **Файл:Winpooch_0.6.4_Processes.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/9c/Winpooch_0.6.4_Processes.png *Лицензия:* GPL *Авторы:* ? *Художник:* ?
- **Файл:Zentyal.dashboard.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/6f/Zentyal.dashboard.png *Лицензия:* GPL *Авторы:* http://www.zentyal.org/screenshots *Художник:* Zentyal Development Team
- **Файл:Zentyal_logo.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/c/c9/Zentyal_logo.jpg *Лицензия:* Public domain *Авторы:* собственная работа *Художник:* Zentyal
- **Файл:Zillya.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/b/b1/Zillya.png *Лицензия:* Добросовестное использование *Авторы:* http://www.zillya.com/img/main_window_ru.png *Художник:* ООО «Олайти Сервис»
- **Файл:Zillya_tm.jpg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/7/74/Zillya_tm.jpg *Лицензия:* Public domain *Авторы:* http://zillya.com/en/zillya_antivirus.html *Художник:* ALLIT Service LLC
- **Файл:ZoneAlarm.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/4/42/ZoneAlarm.png *Лицензия:* Добросовестное использование *Авторы:* Скриншот программы *Художник:* Check Point Software Technologies
- **Файл:cce_intro.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/c/c8/Cce_intro.png *Лицензия:* Добросовестное использование *Авторы:* http://help.comodo.com/uploads/Comodo%20Cleaning%20Essentials/bb4c540dfb2ed5b8e89391c737a4f62d/5eac818f1e1c4adc19d335055b06586b/7e385a926d99a635f2b753a64b280573/cce_intro.png *Художник:* Comodo Group
- **Файл:cce_logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/2/20/Cce_logo.png *Лицензия:* Добросовестное использование *Авторы:* http://www.comodo.com/images/product-icons/cce_logo.png *Художник:* Comodo Group
- **Файл:littlesnitch.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/d/d6/Littlesnitch.png *Лицензия:* Добросовестное использование *Авторы:* http://www.obdev.at/products/littlesnitch/ *Художник:* Objective Development Software GmbH
- **Файл:netfilter-logo.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/6/6b/Netfilter-logo.png *Лицензия:* Добросовестное использование *Авторы:* http://www.netfilter.org/images/netfilter-logo2.png *Художник:* Shane Chan, Pablo Neira Ayuso

- **Файл:Коробка_программы_ИКС.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/c/c4/%D0%9A%D0%BE%D1%80%D0%BE%D0%B1%D0%BA%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B_%D0%98%D0%9A%D0%A1.png *Лицензия:* CC BY-SA 3.0 *Авторы:* собственная работа *Художник:* Sun4wind
- **Файл:Логотип_Dr.Web.png** *Источник:* https://upload.wikimedia.org/wikipedia/ru/3/32/%D0%9B%D0%BE%D0%B3%D0%BE%D1%82%D0%B8%D0%BF_Dr.Web.png *Лицензия:* Добросовестное использование *Авторы:* http://vk.com/drwebuser *Художник:* Dr. Web

100.3.3. Лицензия

- Creative Commons Attribution-Share Alike 3.0