Сравнение антивирусного программного обеспечения

Васильев Михаил Владимирович

Студент 4 курса Московского Физико-Технического Института,

физтех-школа "Радиотехника и компьютерные технологии"

Россия, г.Долгопрудный.

(Dated: 5 декабря 2022 г.)

I. Аннотация

Проведён сравнительный анализ функциональных возможностей различного антивирусного программного обеспечения. Описана общепринятая методика сравнительного тестирования антивирусных продуктов. Проведено сопоставление общепринятой методики с результатами российских учёных.

II. Введение

В настоящее время существует большое количество антивирусных программ и их методов тестирования, а следовательно, практически любая антивирусная программа (АП) может быть лучшей по результатам проверки. Ключевой проблемой конечного пользователя является выбор оптимального защитного ПО. Целью данного эссе является описание универсальных методов оценки АП, а также применение их для нахождения лучшего решения на рынке.

III. Необходимость установки антивирусной программы

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

Ключевой особенностью антивирусной защиты является то, что количество и качество вирусов меняется каждый день. Математически доказано, что ни одна технология не может защитить конечное устройство на 100%. Пользователю необходимо самостоятельно подбирать продукты на рынке. Ситуация осложняется тем, что практически каждый производитель антивирусного ПО может заявлять, что его программа лучшая. Причиной данной проблемы является не обман потребителя, а множество методов проверки качества продукции. Несмотря на это приобретение оптимального защитного решения совершенно необходимо каждому пользователю персонального компьютера.

IV. Принцип действия АП

Базируется в основном на 4 подходах к поиску вредоносных программ:

Метод поиска сигнатур – основан на анализе существующих вирусов и выделении уникального битового кода (сигнатуры) характерного для определённой программы. После чего сигнатура заносится в специальную базу данных. Постоянное обновление этой базы данных позволяет антивирусным программам поддерживать свою эффективность.

Ключевым преимуществом данного метода является малое количество ложных срабатываний, а недостатком – принципиальная невозможность нахождения новых угроз.

Метод контроля целостности – рассматривает неожиданное и беспричинное изменение данных на диске как сигнал подозрительной активности вредоносных программ. Факт нарушения целостности данных легко и быстро проверяется путём сравнения уже посчитанной контрольной суммы с настоящей. Если они не совпадают производится дополнительная проверка на совпадения вирусных сигнатур исполняемой программы и базы данных. Преимуществами данного метода являются: быстрота, так как проверка контрольных сумм занимает меньше времени, и возможность нахождения ранее неизвестных вирусов.

Метод сканирования подозрительных команд – выявляет в программах признаки подозрительных команд и битовых последовательностей. После этого производятся дополнительные действия по проверке файла. Этот подход часто не способен выявлять новые угрозы.

Метод отслеживания поведения программ – основан на анализе поведения запущенных программ. Для него необходимо активное присутствие человека, для подтверждения действий антивируса. Так как при наличии большого количества ложных срабатываний пользователь склонен к выбору оптимистичного сценария, часто используется режим эмулятора работы программы. Данный метод показал свою высокую эффективность в борьбе с известными и неизвестными вирусами.

Брандмауэр или сетевой экран - предназначен для защиты от сетевых. Многие программы для соединения с удаленными компьютерами или серверами могут использовать небезопасные методы, оставляя уязвимости для проникновения извне. Суть работы брандмауэра в контроле как входящего, так и исходящего трафика пу-

тем ограничения возможности устанавливать соединения с определенными удаленными ресурсами. Самый наглядный метод защиты – белые и черные списки сетевых ресурсов. Черный список сетевых ресурсов – это список, например, сайтов, куда заходить нельзя, а белый список – это список ресурсов, куда только и можно заходить. Настройки брандмауэра позволяют обеспечить возможность сетевого взаимодействия только с проверенными ресурсами, отсекая все потенциально опасные и непроверенные. Недостаток брандмауэра вытекает из его достоинства: для качественной настройки файрвола требуются хорошие знания сетевых протоколов и особенностей работы сетевых приложений. Брандмауэр, работающий с настройками «по умолчанию» мало от чего способен защитить.

Почтовый Антивирус - проверяет входящие и исходящие сообщения электронной почты на наличие в них вирусов и других программ, представляющих угрозу. Он запускается при старте, постоянно находится в оперативной памяти компьютера и проверяет все сообщения, получаемые или отправляемые.

Антиспам — позволяет фильтровать почту от нежелательных писем. Зачастую подобные сообщения могут обладать вредоносными программами.

Родительский контроль — программа в Интернете для предотвращения его предполагаемого негативного воздействия на ребёнка.

Резервное копирование — процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

VPN (виртуальная частная сеть) — позволяет создать безопасное зашифрованное подключение между несколькими устройствами поверх уже работающей сети. Благодаря ей пользователи могут получить удаленный доступ к закрытым сетям, а также замаскировать свой трафик и действия в интернете.

V. Решения на рынке

Kaspersky Internet Security

Один из самых популярных программных продуктов, созданный лабораторией Касперского входящей в четвёрку ведущих мировых производителей программного обеспечения для защиты устройств. Предназначен прежде всего для пользователей опера-

ционной системы Windows. Существуют как базовые виды защиты, так и улучшенные решения (Kaspersky Internet security, Total Security). Основными преимуществами данного решения являются: антивирусные базы, которые регулярно обновляются, лёгкость в установке, отсутствие проблем с приобретением и оплатой подписки в связи с санкционной политикой запада.

McAfee

Представляет собой антивирусное программное обеспечение американского разработчика McAfee Incorporated, которое работает с наиболее популярными операционными системами (Windows, Mac, Android). Плюсом является наличие бесплатной демо версии. Удобный интерфейс, достойный уровень защиты, малое время проверки на вирусы и обновление баз данных в автоматическом режиме выгодно отличают данное решение от других.

Dr. Web Security Space

Создан российской компанией «Доктор Веб» и считается первой созданной антивирусной программой в мире. Этот продукт совместим с Windows и Android платформами. Отличительной особенностью является то, что данная программа для проведения анализа пользовательских данных не загружает их к себе на сервера, что говорит о ее хорошем уровне защиты. Автоматическое обновление баз данных вирусных носителей происходит каждый день. Сама программа работает на уровне ядра операционной системы.

Avira Antivir

Является антивирусной комплексной программой, созданной немецкой компанией Avira GmbH, которая более тридцати лет работает в сфере информационной безопасности. Продукт отлично совместим с основными операционными программами, прост в использовании и имеет бесплатную тестовую версию сроком действия до тридцати дней. Есть возможность настроить параметры под пользователя (отключение автозапуска, автоматическое или ручное управление). При обнаружении зараженного файла, система сразу его стирает с носителя инфорации без помещения в карантин.

Norton Security

Это разработка американской компании Symantec, которая является лидером в создании программного обеспечения. Данный антивирус обладает гибкой системой настроек пользователя под свои нужды (резервное копирование, оп- тимизация простран-

ства на диске, управление автозагрузкой), прост в использовании и имеет хороший уровень технической поддержки. Сам интерфейс удобен и понятен для пользователя.

VI. Анализ функциональных возможностей антивирусных программ

Параметры	Kaspersky Internet Security	McAfee Total Protection	Dr. Web Security Space	Norton Security	Avira Antivir
Файловый антивирус	Да	Да	Да	Да	Да
Почтовый антивирус	Да		Да	Да	Да
Сетевой экран	Да	Да	Да	Да	Да
Интернет антивирус	Да	Да	Да	Да	Да
Анти-спам	Да		Да	Да	
Родительский контроль	Да	Да	Да	Да	Да
Резервное копирование	Да	Да	Да	Да	
Менеджер паролей	Да	Да			Да
Встроенный VPN					Да
Наличие версии для ОС Windows	Да	Да	Да	Да	Да
Наличие версии для ОС Android	Да	Да	Да	Да	Да

VII. Общепринятая методика подбора антивирусного программного обеспечения

Не смотря на обилие методов проверки АП, существует универсальный метод проверки антивирусного ПО. Он основан на деятельности некоммерческой организации

WildList, которая сама тестированиями не занимается, а предоставляет тестерам базы данных диких вирусов. «Дикие вирусы» – это вирусы, свободно распространяющиеся по Всемирной сети и периодически атакующие компьютеры пользователей. Базы данных подобных вирусов обновляются ежемесячно и предоставляются тестирующим компаниям независимо.

AV-Comparatives – один из мировых лидеров в области тестирования ПО для защиты от угроз. По результатам испытаний антивирусным продуктам выдается сертификат Real-World Protection.

В рамках сертификации продукты тестируются по категориям. Сегодня это 4 типа испытаний и, соответственно, 4 типа сертификатов:

• Advanced+ - испытываемый продукт должен распознать все вирусы из списка «In The Wild», выпущенного за два месяца до даты тестирования.

• Advanced - антивирус, получивший этот сертификат, должен не только обнаружить, но и вылечить систему от всех вирусов, найденных в Level 1.

• Standard – средний уровень защиты.

• Tested – тест не был пройден.

Таблица результатов:

Антивирус	Оценка
Kaspersky Internet Security	Advanced +
McAfee Total Protection	Advanced +
Dr. Web Security Space	Нет данных
Norton Security	Advanced + (2019)
Avira Antivir	Advanced +

По данным видно, что Kaspersky, McAfee и Aviva прошли испытания AV-Comparatives на высший балл. Тогда как Norton не проходил испытания в 2020 и 2021 годах. Dr.Veb в последнее время вообще в испытаниях участия не принимал.

VIII. Методология проверки антивирусного ПО российскими учёными

Проверка распространённых антивирусных программ проводится не только за рубежом, но и в России. Для этой цели комманда Anti-Malware.ru провела серию исследова-

ний и разработала перечень критериев по данной тематике. Далее описана методология проверки.

В каждом тестируемом антивирусе запускалась задача сканирования по требованию каталога с огромным количеством вирусных экземпляров. Тестовая база вирусов состояла из 64446 программ. Коллекция сформирована путем поиска в Интернете. Также все тестируемые программы на момент тестирования имели актуальные версии с обновленными базами данных.

Для проведения тестирования антивирусов на лечение активного заражения экспертной группой отбирались вредоносные программы по следующим критериям:

1. детектирование родительского файла всеми участвующими в тесте антивирусами;

2. способность маскировать свое присутствие;

3. способность противодействовать обнаружению со стороны антивируса;

4. способность восстанавливаться в случае удаления некоторых компонент;

5. распространенность и известность;

Отбор состоял из выбора наиболее сложных примеров, которые удовлетворяют всем приведённым выше примерам. Детектирование вирусов со стороны всех участвовавших в тести антивирусов было критически важным параметром для выбора вредоностных программ. Все используемые в тесте вредоносные программы были собраны экспертами во время распространения в Интернет (In The Wild). Каждый отобранный экземпляр вредоносной программы проверялся на работоспособность и установку на тестовой системе.

Следующая таблица приводит результаты тестрования наиболее популярных антивирусов:

Наименование	Всего	Вирусов	% опознанных	Позиция в рейтинге
McAfee Total Protection	65169	62605	96	1
Dr. Web Security Space	86190	59621	69	2
Avira Antivir	76919	47552	62	3
Kaspersky Internet Security	109490	67205	61	4
Norton Security	84427	37015	44	5

IX. Вывод

В данном эссе было представлено три различных независимых подхода к оценке антивирусных программ. Для конечного пользователя представляет интерес функциональный анализ и сертификация AV-Comparatives. По результатам данного исследования можно сказать, что при прочих равных выбор можно отдать McAfee.

X. Источники

https://cyberleninka.ru/article/n/razrabotka-metodiki-sravnitelnogo-testirovaniya-antivirusnyh-produktov/viewer

https://cyberleninka.ru/article/n/sravnitelnyy-analiz-antivirusnogo-programmnogo-obespecheniya/viev

https://cyberleninka.ru/article/n/kompyuternye-virusy-i-antivirusy/viewer

https://www.av-comparatives.org/tests/real-world-protection-test-july-october-2022/

https://support.kaspersky.com/KESWin/10SP2/ru-RU/128014.htm