Министерство сельского хозяйства Российской Федерации
ФГБОУ ВО Рязанский государственный агротехнологический университет имени П.А. Костычева

Инженерный факультет

РЕФЕРАТ

по дисциплине
«Информатика»
на тему:
«Классификация и особенности современных программ защиты информации»

Выполнил:
студент 1 курса
инженерного факультета
специальности
Электроэнергетика и
электротехника группы
ИО3105 Денисов
Александр Игоревич

Проверил:
доцент кафедры,
к.э.н. Романова Л.В.

Рязань 2022

Содержание

Введение

В наш век многие сферы человеческой деятельности связаны с использованием компьютеров. Эти машины стали неотъемлемой частью нашей жизни. Они обладают колоссальными возможностями и, таким образом, позволяют освободить человеческий мозг для более необходимых и ответственных задач. Компьютер может хранить и обрабатывать очень большое количество информации, что на сегодняшний день является одним из самых дорогих ресурсов. По мере развития и модернизации компьютерных систем и программного обеспечения увеличивается объем и уязвимость хранимых в них данных. Одним из новых факторов, значительно увеличивших уязвимость, является массовое производство программно-совместимых, высокопроизводительных персональных компьютеров, что стало одной из причин появления нового класса программного обеспечения — вандалов — компьютерных вирусов. Наибольшую опасность в результате риска заражения компьютерными вирусами представляет возможность искажения или уничтожения жизненно важной информации, что может привести не только к финансовым и временным потерям, но и к человеческим потерям. антивирус компьютерной программы

Компьютерные вирусы очень распространены, и борьба с ними вызывает у среднего пользователя большие «головные боли». Поэтому важно понимать, как распространяются вирусы и как с ними бороться.

Наилучшие результаты в настоящее время достигаются в разработке антивирусных программ и методов их применения. Ряд разработок был доведен до уровня программных продуктов и широко используется пользователями.

1.Виды антивирусных программ

Рисунок 1.1.

Антивирусная программа (антивирус) — любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком. Имеются различные типы антивирусных программ – полифаги, ревизоры, блокировщики, сторожа, вакцины и пр.

Различают следующие виды антивирусных программ: взятых с учебной библиотеки ЭБС Лань (lanbook.com).

1. Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

2. Программы-доктора (фаги) не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

3. Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

4. Программы-фильтры (сторожа) представляют собой небольшие резидентные программы, предназначенные для

обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

5. Программы-вакцины (иммунизаторы) - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Также все описания программ-антивирусников были взяты интернет сточников, такие как ИНФОУРОК, МУЛЬТИУРОК, википедия, видеурок.нет.

1.1 Программы – детекторы.

Программ-детекторы рассчитаны на обнаружение конкретных вирусов и основаны на сравнении характерной (спецификой) последовательности байтов (сигнатур или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ. Программы – детекторы нужно регулярно обновлять, так как они быстро устаревают и не могут выявлять новые виды вирусов.

Следует подчеркнуть, что программы – детекторы могут обнаружить только те вирусы, которые ей “известны”, то есть, сигнатуры этих вирусов заранее помещены в библиотеку антивирусных программ.

Таким образом, если проверяемая программа не опознается детектором как зараженная, то еще не следует считать, что она “здорова”. Она может быть инфицирована новым вирусом, который не занесен в базу данных детектора.

Для устранения этого недостатка программы – детекторы стали снабжаться блоками эвристического анализа программ. В этом режиме делается попытка обнаружить новые или неизвестные вирусы по характерным для всех вирусов кодовым последовательностям. Наиболее развитые эвристические механизмы позволяют с вероятностью около 80% обнаружить новый вирус.

Теперь рассмотрим представителя программ-детекторы **Dr.Web** –антивирус российского производства, кстати, сертифицированный Министерством обороны Российской Федерации. Если говорить о функциях защиты, то они во многом схожи с антивирусом Касперского, да и с функциями многих других популярных продуктов, таких как Nod32, Norton, Panda, но только реализованные под другой графической оболочкой.

Помимо модулей антивируса, антишпиона, антируткита, антиспама, веб-антивируса и брандмауэра, имеющихся во всех продуктах Dr.Web, Dr.Web Бастион Pro предлагает функцию Криптограф, предназначенную для шифрования информации в специальных файловых контейнерах. Также как и в «Касперском», есть возможность активировать пробную версию на 30 дней, но с той лишь разницей, что эту процедуру можно повторять один раз в четыре месяца.

Бесплатная для домашнего использования утилита Dr.Web CureIt! не защищает ПК в реальном времени, зато позволяет без

установки просканировать систему на наличие вредоносного программного обеспечения.

Если компьютер заражен настолько, что даже запуск Windows или Unix проблематичен, то на помощь придет Dr.Web LiveCD – диск аварийного восстановления системы. С помощью него Вы легко восстановите работоспособность пораженной системы совершенно бесплатно! Dr.Web LiveCD поможет не только очистить компьютер от инфицированных и подозрительных файлов, но и скопировать важную информацию на сменные носители или другой компьютер, а также попытается вылечить зараженные объекты.

1.2. Программы – доктора

Программы-доктора или фаги находят зараженные вирусами файлы и «лечат» их, удаляя из файла тело программы-вируса, возвращая файлы в исходное состояние. Программы-доктора, позволяющие лечить большое число вирусов, называются полифагами.

В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов.

Наибольшее распространение в нашей стране получили программы-детекторы, а вернее программы, объединяющие в себе детектор и доктор. Наиболее известные представители этого класса – Aidstest, Doctor Web, Microsoft AntiVirus.

Постоянно появление новых вирусов, требует регулярное обновление версий программ-детекторов и программ-докторов, в связи с их быстрым устареванием.

Примером такой программы-доктора служит антивирусная программа Doctor Web.

Рисунок 1.2.1. антивирусная программа Doctor Web.

"Лечебная паутина" Doctor Web относится к классу детекторов-докторов и имеет "эвристический анализатор" - алгоритм, позволяющий обнаруживать неизвестные вирусы. Doctor Web содержит антивирус, антируткит, антишпион и сетевой брандмауэр.

Основное достоинство антивируса Doctor Web это большой процент излечения пораженных файлов. Но нет стопроцентной гарантии, что при сканировании памяти "Лечебная паутина" обнаружит все вирусы.

Пользователь может указать программе тестировать как весь диск, так и отдельные подкаталоги или группы файлов, или же отказаться от проверки дисков и тестировать только оперативную память. Doctor Web может создавать отчет о работе.

Doctor Web обладает технологиями лечения неизвестных угроз, может проверить и вылечить архив любого уровня вложенности, а также нейтрализовать вирусы, которые существуют только в оперативной памяти компьютера.

Антивирус Касперского давно завоевал популярность у миллионов пользователей благодаря своей эффективности и быстроте реакции на различные угрозы. Несмотря на все свои преимущества, до сих пор многие не знающие товарищи критикуют его за то, что он якобы очень сильно нагружает систему. Так было в недалёких 2003-2004 годах, тогда многие антивирусные продукты не особо выделялись «лёгкостью». Теперь совсем другие времена и одним из главных требований к современным антивирусам является небольшое потребление ресурсов компьютера, хотя стоит заметить, что если дать команду на полное и глубокое сканирование, то для этого будет задействованы все средства, зато в других случаях система остаётся почти незатронутой.

Рисунок 1.2.2. Антивирус Касперского.

Последними версиями являются антивирус Касперского 2010, комплексная защита Kaspersky Internet Security 2010 и Kaspersky CRYSTAL.

Антивирус Касперского 2010 обладает всеми основными функциями защиты, вот некоторые из них: классический антивирус, антишпионский модуль, онлайн сканер и веб-антивирус, защищающий в режиме реального времени при просмотре Интернет страниц. Имеется новая функция – виртуальная клавиатура, позволяющая безопасно вводить данные и не бояться программ, крадущих логины и пароли.

В Kaspersky Internet Security 2010 присутствуют те же функции, плюс есть наличие сетевого экрана, защищающего от внешних вторжений из Интернета. Kaspersky CRYSTAL в отличии от Kaspersky Internet Security 2010 оснащён ещё и функцией резервного копирования и восстановления данных.

Также в продуктах лаборатории Касперского присутствует функция Родительского контроля, ограждающая детей от посещения нежелательных Интернет сайтов. Учитывая наличие мощной защиты в данном продукте, не стоит удивляться его цене. К примеру, лицензия Kaspersky CRYSTAL для 2-х компьютеров стоит около 88у.е., а остальные версии, ввиду отсутствия некоторых функций, стоят немного дешевле. Прежде чем приобретать какую-либо версию, лучше скачать установочный дистрибутив с официального сайта и установить пробную версию продукта, которая будет доступна 30 дней.

1.3. Ревизоры.

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.

Ревизоры (**AVG**)– это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние BOOT – сектора, FAT – таблицы, а также длина файлов, их время создания, атрибуты, контрольные суммы. Контрольная сумма является интегральной оценкой всего

файла (его слепком). Получается контрольная сумма путем суммирования по модулю для всех байтов файла. Практически всякое изменение кода программы приводит к изменению контрольной суммы файла.

Рисунок 1.3.1. Ревизоры (AVG)

AVG Antivirus, AVG Anti-Virus — антивирусная система производства чешской компании AVG Technologies, имеющая сканер файлов, сканер электронной почты и поддерживающая возможность автоматического наблюдения. Система безопасности AVG сертифицирована всеми главными независимыми сертификационными компаниями, такими как ICSA, AV-TEST, Virus Bulletin, Checkmark (лаборатория West Coast Labs)

1.4. Антивирусы – фильтры

Антивирусы – фильтры – это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой – либо программы выполнить подозрительные действия. Фильтры контролируют следующие операции:

Обновление программных файлов и системной области диска;

Форматирование диска;

Резидентное размещение программ в ОЗУ.

Антивирусы-фильтры или сторожа. Программы, уведомляющие пользователя, если троянская программа или вирус захотят проникнуть на ваш ПК или, наоборот, украсть пароль и отправить его злоумышленнику, сторож мгновенно сработает и спросит: «Разрешить или запретить выполнение операции?». К сожалению, работа с данным типом защиты требует определённых навыков, ведь далеко не каждый пользователь знает, что обозначает тот или иной процесс. Вдруг это Windows вздумала обновиться, а сторож её фильтрует?

Антивирус-фильтр есть практически на каждом ПК и называется он брандмауэр. Если стандартный сторож не устраивает пользователя, он может приобрести что-нибудь по-круче, например, Outpost Security Suite или Agnitum Outpost Firewall. Многие современные антивирусы имеют встроенный брандмауэр, позволяющий контролировать сетевой трафик и следить за изменениями в системе.

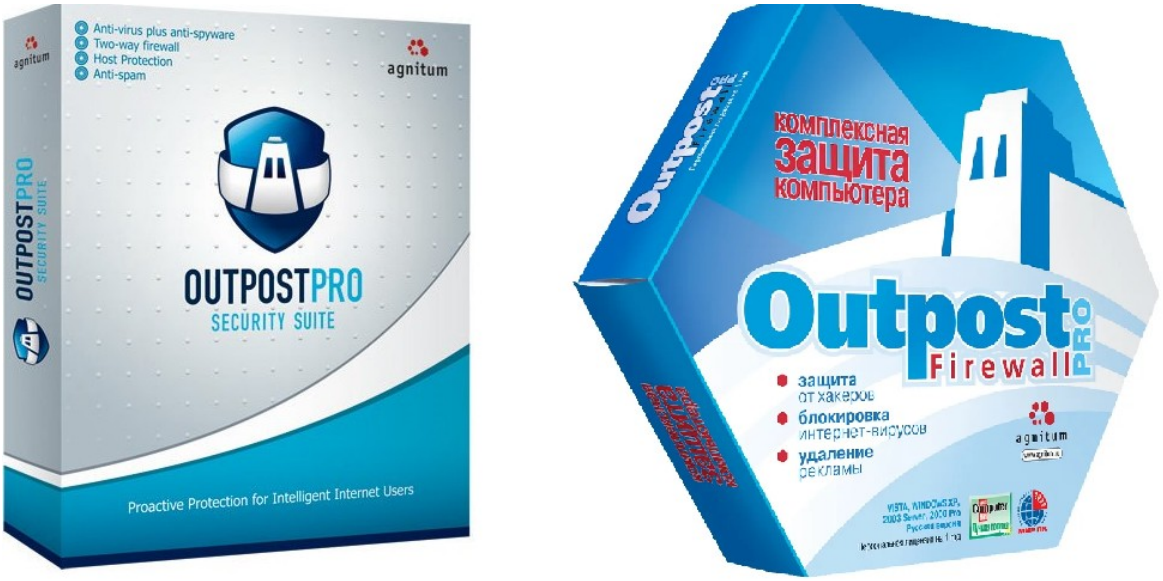

Рисунок 1.4.1. Антивирус-фильтр Outpost Security Suite и Agnitum Outpost Firewall.

1.5. Вакцинаторы (иммунизаторы).

Вакцинаторы (иммунизаторы) предотвращают заражение файлов только известными вирусами. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время вакцины редко применяются, так как имеют ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Наиболее распространены программы доктора и фильтры. А современные антивирусные пакеты включают все необходимые компоненты для противостояния любым вирусам. Например, «Антивирус Касперского» (Kaspersky Anti-Virus) содержит программу-фильтр Kaspersky Anti-Virus Monitor, доктор Kaspersky Anti-Virus Scanner и ревизор Kaspersky Anti-Virus Inspector.

Несмотря на широкую распространенность антивирусных программ, вирусы продолжают «плодиться». Чтобы справиться с ними, необходимо создавать более универсальные и качественно-новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. Защищенность от вирусов зависит и от грамотности пользователя. Применение вкупе всех видов защит позволит достигнуть высокой безопасности компьютера и, соответственно, информации.

Из всех вышеперечисленный ативирусных программ самые популярные, безлопастные и эффективные: Kaspersky, Avast, Dr.Web, ESET NOD32, AVG, McAfee, ZoneAlarm.

Диаграмма1.Рейтинг пользования антивирусниками.


Пользование антивирусниками
Kaspersky
Dr.Web
AVG
McAfee
Outpost Security Suite
Agnitum Outpost Firewall
Punda
WedBroot
Malwarebets
11%
13%
15%
14%
16%
12%
13%
3%
3%

Заключение

Компьютерные вирусы во всем мире наносят громадный ущерб. Эти маленькие вредоносные программы живут по трём правилам – Размножаться, Скрываться и Портить. И какие потрясения бывают, когда однажды пропадают данные, которые собирались и накапливались может не один год....

Чтобы этого не произошло, нужно знать о существовании компьютерных вирусов и уметь защищать свои данные.

Хорошая антивирусная программа должна:

Обеспечивать эффективную защиту в режиме реального времени. Производить проверку всех файловых операций, сообщений электронной почты, данных и программ, получаемых из Интернета. Позволять проверять все содержимое локальных дисков "по требованию", запуская проверку вручную или автоматически по расписанию. Защищать наш компьютер даже от неизвестных вирусов. Уметь проверять и лечить архивированные файлы. Давать возможность ежедневно обновлять антивирусные базы.

И все-таки, какой антивирус лучше поставить? Ведь, самый главный критерий комфорта работы с ПК - его безопасность.

Каждый из рассмотренных антивирусов по тем или иным показателям заслужил свою популярность, но явного лидера среди них выявить невозможно.

Для своего компьютера, самый лучший антивирус следует подбирать, исходя из функциональности, самостоятельно протестировав несколько продуктов. Многие разработчики антивирусных программ предлагают возможность использовать

бесплатную пробную версию (от 30 до 90 дней). Это позволит и ознакомиться с продуктом, понять, какой антивирус самый лучший именно для вас, и потратить деньги только на программу, отвечающую всем необходимым запросам, которая заслужит ваше доверие.

К сожалению, на данный момент универсальной антивирусной программы не существует. Существующие антивирусные программы способны защитить информацию, хранящуюся на компьютере. Но ни одна из них не может гарантировать нам 100% защиты от вирусов, и во многом выбор антивирусной программы зависит от самого пользователя.

Антивирус вещь хорошая, но некоторые пользователи умудряются заразить компьютер даже с ним, поэтому, нужно помнить прописную истину пользователя: «Если не знаешь, что это, откуда и для чего, лучше не открывай!».

Список литературы

- Лань-Антивирусная защита компьютерных систем, издатель-Национальный Открытый Университет "ИНТУИТ", 2016.
- «Зачем тебе антивирус?» — Статья из «Помощи джунглям».
- «Антивирусная программа». Материал из Википедии — бесплатная энциклопедия.
- Ф.Файтс, П.Джонстон, М.Кратц "Компьютерный вирус: проблемы и прогноз". Москва, "Мир", 2020 г.
- Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. – М.: «СОЛОН-Р», 2001.

Интернет- ресурсы

- http://journal-shkolniku.ru/komputer-virus.html
- http://www.comss.ru/page.php?id=1799
- http://www.comss.ru/page.php?id=457
- http://www.softroad.ru/articles/reviews/73-virus-history.html
- http://www.esetnod32.ru/company/press/center/obzor-informatsionnykh-ugroz-yanvarya-2014-goda/
- Сайт «Лаборатория Касперского» - http://www.kaspersky.ru/