**Содержание**

Введение

1. Теоретическая часть

1.1 Понятие защиты информации

1.2 Виды угроз

1.3 Методы защиты информации

2. Проектная часть

2.1 Классификация компьютерных вирусов

2.2 Понятие антивирусной программы

2.3 Виды антивирусных средств

2.4 Сравнение антивирусных пакетов

Заключение

Список использованной литературы

Приложение

**Введение**

Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность не только становится обязательной, она еще и одна из характеристик информационных систем. Существует довольно обширный класс систем обработки информации, при разработке которых фактор безопасности играет первостепенную роль.

Массовое применение персональных компьютеров связано с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

С каждым днем вирусы становятся все более изощренными, что приводит к существенному изменению профиля угроз. Но и рынок антивирусного программного обеспечения не стоит на месте, предлагая множество продуктов. Их пользователи, представляя проблему лишь в общих чертах, нередко упускают важные нюансы и в итоге получают иллюзию защиты вместо самой защиты.

Целью данной курсовой работы является проведение сравнительного анализа антивирусных пакетов.

Для достижения этой цели в работе решаются следующие задачи:

- изучить понятия информационной безопасности, компьютерных вирусов и антивирусных средств;

- определить виды угроз безопасности информации, методы защиты;

- изучить классификацию компьютерных вирусов и антивирусных программ;

- провести сравнительный анализ антивирусных пакетов;

- создать программу-антивирус.

Практическая значимость работы.

Полученные результаты, материал курсовой работы можно использовать как основу для самостоятельного сравнения антивирусных программ.

Структура курсовой работы.

Данная курсовая работа состоит из Введения, двух разделов, Заключения, списка используемой литературы.

компьютерный вирус безопасность антивирусный

**1. Теоретическая часть**

В процессе проведения сравнительного анализа антивирусных пакетов необходимо определить следующие понятия:

1 Информационная безопасность.

2 Виды угроз.

3 Методы защиты информации.

Перейдем к подробному рассмотрению этих понятий:

**1.1 Понятие защиты информации**

Несмотря на все возрастающие усилия по созданию технологий защиты данных их уязвимость в современных условиях не только не уменьшается, но и постоянно возрастает. Поэтому актуальность проблем, связанных с защитой информации все более усиливается.

Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Например, конфиденциальность данных, которая обеспечивается применением различных методов и средств. Перечень аналогичных задач по защите информации может быть продолжен. Интенсивное развитие современных информационных технологий, и в особенности сетевых технологий, создает для этого все предпосылки.

Защита информации – комплекс мероприятий, направленных на обеспечение целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

На сегодняшний день сформулировано два базовых принципа по защите информации:

1 целостность данных – защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания или уничтожения данных;

2 конфиденциальность информации.

Защита от сбоев, ведущих к потере информации, ведется в направлении повышения надежности отдельных элементов и систем, осуществляющих ввод, хранение, обработку и передачу данных, дублирования и резервирования отдельных элементов и систем, использования различных, в том числе автономных, источников питания, повышения уровня квалификации пользователей, защиты от непреднамеренных и преднамеренных действий, ведущих к выходу из строя аппаратуры, уничтожению или изменению (модификации) программного обеспечения и защищаемой информации.

Защита от неавторизованного создания или уничтожения данных обеспечивается физической защитой информации, разграничением и ограничением доступа к элементам защищаемой информации, закрытием защищаемой информации в процессе непосредственной ее обработки, разработкой программно-аппаратных комплексов, устройств и специализированного программного обеспечения для предупреждения несанкционированного доступа к защищаемой информации.

Конфиденциальность информации обеспечивается идентификацией и проверкой подлинности субъектов доступа при входе в систему по идентификатору и паролю, идентификацией внешних устройств по физическим адресам, идентификацией программ, томов, каталогов, файлов по именам, шифрованием и дешифрованием информации, разграничением и контролем доступа к ней.

Среди мер, направленных на защиту информации основными являются технические, организационные и правовые.

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и так далее.

К организационным мерам относятся: охрана вычислительного центра (кабинетов информатики); заключение договора на обслуживание компьютерной техники с солидной, имеющей хорошую репутацию организацией; исключение возможности работы на компьютерной технике посторонних, случайных лиц и так далее.

К правовым мерам относятся разработка норм, устанавливающих ответственность за вывод из строя компьютерной техники и уничтожение (изменение) программного обеспечения, общественный контроль над разработчиками и пользователями компьютерных систем и программ.

Следует подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных системах. В то же время свести риск потерь к минимуму возможно, но лишь при комплексном подходе к защите информации.

**1.2 Виды угроз**

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов информационной системы, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и так далее.

Активные угрозы имеют целью нарушение нормального функционирования информационной системы путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например, вывод из строя компьютера или его операционной системы, разрушение программного обеспечения компьютеров, нарушение работы линий связи и так далее. Источником активных угроз могут быть действия взломщиков, вредоносные программы и тому подобное.

Умышленные угрозы подразделяются также на внутренние (возникающие внутри управляемой организации) и внешние.

Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом.

Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями).

К основным угрозам безопасности информации и нормального функционирования информационной системы относятся:

- утечка конфиденциальной информации;

- компрометация информации;

- несанкционированное использование информационных ресурсов;

- ошибочное использование информационных ресурсов;

- несанкционированный обмен информацией между абонентами;

- отказ от информации;

- нарушение информационного обслуживания;

- незаконное использование привилегий.

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы информационной системы или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

- разглашения конфиденциальной информации;

- ухода информации по различным, главным образом техническим, каналам;

- несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

- перехват электронных излучений;

- принудительное электромагнитное облучение линий связи с целью получения паразитной модуляции несущей;

- применение подслушивающих устройств;

- дистанционное фотографирование;

- перехват акустических излучений и восстановление текста принтера;

- копирование носителей информации с преодолением мер защиты;

- маскировка под зарегистрированного пользователя;

- маскировка под запросы системы;

- использование программных ловушек;

- использование недостатков языков программирования и операционных систем;

- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ информации;

- злоумышленный вывод из строя механизмов защиты;

- расшифровка специальными программами зашифрованной информации;

- информационные инфекции.

Перечисленные пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, используются технические каналы утечки – это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений. Причиной возникновения каналов утечки являются конструктивные и технологические несовершенства схемных решений либо эксплуатационный износ элементов. Все это позволяет взломщикам создавать действующие на определенных физических принципах преобразователи, образующие присущий этим принципам канал передачи информации – канал утечки.

Однако есть и достаточно примитивные пути несанкционированного доступа:

- хищение носителей информации и документальных отходов;

- инициативное сотрудничество;

- склонение к сотрудничеству со стороны взломщика;

- выпытывание;

- подслушивание;

- наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует информационная система, так и для ее пользователей.

Существует и постоянно разрабатывается огромное множество вредоносных программ, цель которых – порча информации в базах данных и программном обеспечении компьютеров. Большое число разновидностей этих программ не позволяет разработать постоянных и надежных средств защиты против них.

Вирус – программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению.

Считается, что вирус характеризуется двумя основными особенностями:

- способностью к саморазмножению;

- способностью к вмешательству в вычислительный процесс (к получению возможности управления).

Несанкционированное использование информационных ресурсов, с одной стороны, является последствиями ее утечки и средством ее компрометации. С другой стороны, оно имеет самостоятельное значение, так как может нанести большой ущерб управляемой системе или ее абонентам.

Ошибочное использование информационных ресурсов будучи санкционированным тем не менее может привести к разрушению, утечке или компрометации указанных ресурсов.

Несанкционированный обмен информацией между абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен. Последствия – те же, что и при несанкционированном доступе.

**1.3 Методы защиты информации**

Создание систем информационной безопасности основывается на следующих принципах:

1 Системный подход к построению системы защиты, означающий оптимальное сочетание взаимосвязанных организационных, программных,. Аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

2 Принцип непрерывного развития системы. Этот принцип, являющийся одним из основополагающих для компьютерных информационных систем, еще более актуален для систем информационной безопасности. Способы реализации угроз информации непрерывно совершенствуются, а потому обеспечение безопасности информационных систем не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования систем информационной безопасности, непрерывном контроле, выявлении ее узких и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа,

3 Обеспечение надежности системы защиты, то есть невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей и обслуживающего персонала.

4 Обеспечение контроля за функционированием системы защиты, то есть создание средств и методов контроля работоспособности механизмов защиты.

5 Обеспечение всевозможных средств борьбы с вредоносными программами.

6 Обеспечение экономической целесообразности использования системы. Защиты, что выражается в превышении возможного ущерба от реализации угроз над стоимостью разработки и эксплуатации систем информационной безопасности.

В результате решения проблем безопасности информации современные информационные системы должны обладать следующими основными признаками:

- наличием информации различной степени конфиденциальности;

- обеспечением криптографической защиты информации различной степени конфиденциальности при передаче данных;

- обязательным управлением потоками информации, как в локальных сетях, так и при передаче по каналам связи на далекие расстояния;

- наличием механизма регистрации и учета попыток несанкционированного доступа, событий в информационной системе и документов, выводимых на печать;

- обязательным обеспечением целостности программного обеспечения и информации;

- наличием средств восстановления системы защиты информации;

- обязательным учетом магнитных носителей;

- наличием физической охраны средств вычислительной техники и магнитных носителей;

- наличием специальной службы информационной безопасности системы.

Методы и средства обеспечения безопасности информации.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации.

Управление доступом – методы защиты информации регулированием использования всех ресурсов. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

- опознание объекта или субъекта по предъявленному им идентификатору;

- разрешение и создание условий работы в пределах установленного регламента;

- регистрацию обращений к защищаемым ресурсам;

- реагирование при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в информационных системах.

Из средств программного обеспечения системы защиты необходимо выделить еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в информационных системах и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения информации в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные либо оформленные в некий свод правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения.

**2. Проектная часть**

В проектной части необходимо выполнить следующие этапы:

1 Определить понятие компьютерного вируса и классификации компьютерных вирусов.

2 Определить понятие антивирусной программы и классификации антивирусных средств.

3 Провести сравнительный анализ антивирусных пакетов.

**2.1 Классификация компьютерных вирусов**

Вирус – программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению.

Вирусы можно разделить на классы по следующим основным признакам:

- деструктивные возможности

- особенности алгоритма работы;

- среда обитания;

По деструктивным возможностям вирусы можно разделить на:

- безвредные, то есть никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;

- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти

Особенности алгоритма работы вирусов можно охарактеризовать следующими свойствами:

- резидентность;

- использование стелс-алгоритмов;

- полиморфичность;

#### Резидентные вирусы.

Под термином «резидентность» понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Часто от таких вирусов невозможно избавиться восстановлением всех копий файлов с дистрибутивных дисков или backup-копий. Резидентная копия вируса остается активной и заражает вновь создаваемые файлы. То же верно и для загрузочных вирусов – форматирование диска при наличии в памяти резидентного вируса не всегда вылечивает диск, поскольку многие резидентные вирусы заражает диск повторно после того, как он отформатирован.

#### Нерезидентные вирусы. Нерезидентные вирусы, напротив, активны довольно непродолжительное время – только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы. Поэтому файлы, зараженные нерезидентными вирусами значительно проще удалить с диска и при этом не позволить вирусу заразить их повторно.

#### Стелс-вирусы. Стелс-вирусы теми или иными способами скрывают факт своего присутствия в системе. Использование стелс-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение (запись) зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ – запрет вызовов меню просмотра макросов. Известны стелс-вирусы всех типов, за исключением Windows-вирусов – загрузочные вирусы, файловые DOS-вирусы и даже макро-вирусы. Появление стелс-вирусов, заражающих файлы Windows, является скорее всего делом времени.

#### Полиморфик-вирусы. Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы – это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

К полиморфик-вирусам относятся те из них, детектирование которых невозможно осуществить при помощи так называемых вирусных масок – участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами – шифрованием основного кода вируса с непостоянным кличем и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Полиморфизм различной степени сложности встречается в вирусах всех типов – от загрузочных и файловых DOS-вирусов до Windows-вирусов.

По среде обитания вирусы можно разделить на:

- файловые;

- загрузочные;

- макровирусы;

- сетевые.

#### Файловые вирусы. Файловые вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных операционных систем. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной DOS: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы других операционных систем – Windows 3.x, Windows95/NT, OS/2, Macintosh, UNIX, включая VxD-драйвера Windows 3.x и Windows95.

Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств. Макро-вирусы также записывают свой код в файлы данных – документы или электронные таблицы, однако эти вирусы настолько специфичны, что вынесены в отдельную группу.

#### Загрузочные вирусы. Загрузочные вирусы заражают загрузочный (boot) сектор флоппи-диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера – после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление.

В случае дискеты или компакт-диска управление получает boot-сектор, который анализирует таблицу параметров диска (BPB – BIOS Parameter Block) высчитывает адреса системных файлов операционной системы, считывает их в память и запускает на выполнение. Системными файлами обычно являются MSDOS.SYS и IO.SYS, либо IBMDOS.COM и IBMBIO.COM, либо других в зависимости от установленной версии DOS, Windows или других операционных систем. Если же на загрузочном диске отсутствуют файлы операционной системы, программа, расположенная в boot-секторе диска выдает сообщение об ошибке и предлагает заменить загрузочный диск.

В случае винчестера управление получает программа, расположенная в MBR винчестера. Эта программа анализирует таблицу разбиения диска (Disk Partition Table), вычисляет адрес активного boot-сектора (обычно этим сектором является boot-сектор диска C, загружает его в память и передает на него управление. Получив управление, активный boot-сектор винчестера проделывает те же действия, что и boot-сектор дискеты.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, но коду вируса.

Заражение дискет производится единственным известным способом – вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами – вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C, либо модифицирует адрес активного boot-сектора в Disk Partition Table, расположенной в MBR винчестера.

#### Макро-вирусы. Макро-вирусы заражают файлы – документы и электронные таблицы нескольких популярных редакторов. Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки данных. Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла в другие. Наибольшее распространение получили макро-вирусы для Microsoft Word, Excel и Office97. Существуют также макро-вирусы, заражающие документы Ami Pro и базы данных Microsoft Access.

#### Сетевые вирусы. К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла. Пример сетевых вирусов – так называемые IRC-черви.

IRC (Internet Relay Chat) – это специальный протокол, разработанный для коммуникации пользователей Интернет в реальном времени. Этот протокол предоставляет им возможность Итрернет-«разговора» при помощи специально разработанного программного обеспечения. Помимо посещения общих конференций пользователи IRC имеют возможность общаться один на один с любым другим пользователем. Кроме этого существует довольно большое количество IRC-команд, при помощи которых пользователь может получить информацию о других пользователях и каналах, изменять некоторые установки IRC-клиента и прочее. Существует также возможность передавать и принимать файлы – именно на этой возможности и базируются IRC-черви. Мощная и разветвленная система команд IRC-клиентов позволяет на основе их скриптов создавать компьютерные вирусы, передающие свой код на компьютеры пользователей сетей IRC, так называемые «IRC-черви». Принцип действия таких IRC-червей примерно одинаков. При помощи IRC-команд файл сценария работы (скрипт) автоматически посылается с зараженного компьютера каждому вновь присоединившемуся к каналу пользователю. Присланный файл-сценарий замещает стандартный и при следующем сеансе работы уже вновь зараженный клиент будет рассылать червя. Некоторые IRC-черви также содержат троянский компонент: по заданным ключевым словам производят разрушительные действия на пораженных компьютерах. Например, червь «pIRCH.Events» по определенной команде стирает все файлы на диске пользователя.

Существует большое количество сочетаний – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии. Другой пример такого сочетания – сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

В дополнение к этой классификации следует сказать несколько слов о других вредоносных программах, которые иногда путают с вирусами. Эти программы не обладают способностью к самораспространению как вирусы, но способны нанести столь же разрушительный урон.

#### Троянские кони (логические бомбы или временные бомбы).

К троянским коням относятся программы, наносящие какие-либо разрушительные действия, то есть в зависимости от каких-либо условий или при каждом запуске уничтожающая информацию на дисках, «завешивающая» систему, и прочее. В качестве примера можно привести и такой случай – когда такая программа во время сеанса работы в Интернете пересылала своему автору идентификаторы и пароли с компьютеров, где она обитала. Большинство известных троянских коней являются программами, которые «подделываются» под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами «троянские кони» не получают широкого распространения по следующим причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

**2.2 Понятие антивирусной программы**

Способы противодействия компьютерным вирусам можно разделить на несколько групп:

- профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения;

- методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса;

- способы обнаружения и удаления неизвестного вируса.

#### Профилактика заражения компьютера.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того чтобы определить основные правила компьютерной «гигиены», необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office97. Пользователь зараженного макро-вирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и так далее. Следует избегать контактов с подозрительными источниками информации и пользоваться только законными (лицензионными) программными продуктами.

#### Восстановление пораженных объектов.

В большинстве случаев заражения вирусом процедура восстановления зараженных файлов и дисков сводится к запуску подходящего антивируса, способного обезвредить систему. Если же вирус неизвестен ни одному антивирусу, то достаточно отослать зараженный файл фирмам-производителям антивирусов и через некоторое время получить лекарство-«апдейт» против вируса. Если же время не ждет, то обезвреживание вируса придется произвести самостоятельно. Для большинства пользователей необходимо иметь резервные копии своей информации.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

1 Копирование информации – создание копий файлов и системных областей дисков.

2 Разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Главным оружием в борьбе с вирусами являются антивирусные программы. Они позволяют не только обнаружить вирусы, в том числе вирусы, использующие различные методы маскировки, но и удалить их из компьютера.

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программами. Наиболее традиционным методом поиска вирусов является сканирование.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

**2.3 Виды антивирусных средств**

Программы-детекторы. Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора. Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, то есть 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, то есть программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них: AVP, Aidstest, Scan, Norton AntiVirus, Doctor Web.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры (инспектора) относятся к самым надежным средствам защиты от вирусов.

Ревизоры (инспектора) проверяют данные на диске на предмет вирусов-невидимок. Причем инспектор может не пользоваться средствами операционной системы для обращения к дискам, а значит, активный вирус не сможет перехватить это обращение.

Дело в том, что ряд вирусов, внедряясь в файлы (то есть дописываясь в конец или в начало файла), подменяют записи об этом файле в таблицах размещения файлов нашей операционной системы.

Ревизоры (инспектора) 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. Программы-ревизоры (инспектора) имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом.

Запускать ревизора (инспектора) надо тогда, когда компьютер еще не заражен, чтобы он мог создать в корневой директории каждого диска по таблице, со всей необходимой информацией о файлах, которые имеются на этом диске, а также о его загрузочной области. На создание каждой таблицы будет запрошено разрешение. При следующих запусках ревизор (инспектор) будет просматривать диски, сравнивая данные о каждом файле со своими записями.

В случае обнаружения заражений ревизор (инспектор) сможет использовать свой собственный лечащий модуль, который восстановит испорченный вирусом файл. Для восстановления файлов инспектору не нужно ничего знать о конкретном типе вируса, достаточно воспользоваться данными о файлах, сохраненными в таблицах.

Кроме того, в случае необходимости может быть вызван антивирусный сканер.

Программы-фильтры (мониторы). Программы-фильтры (мониторы) или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM, EXE;

- изменение атрибутов файла;

- прямая запись на диск по абсолютному адресу;

- запись в загрузочные сектора диска;

- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги.

Вакцины или иммунизаторы. Вакцины – 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. В настоящее время программы-вакцины имеют ограниченное применение.

Сканер. Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода являетcя алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов. Сканеры также можно разделить на две категории – «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на «резидентные» (мониторы, сторожа), производящие сканирование «налету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как «нерезидентный» сканер способен опознать вирус только во время своего очередного запуска. С другой стороны резидентный сканер может несколько замедлить работу компьютера в том числе и из-за возможных ложных срабатываний.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – относительно небольшую скорость поиска вирусов.

#### CRC-сканеры. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и так далее. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту «слабость» CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них.

Блокировщики. Блокировщики – это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусо-опасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и так далее, то есть вызовы, которые характерны для вирусов в моменты из размножения. Иногда некоторые функции блокировщиков реализованы в резидентных сканерах.

К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения. К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний.

Необходимо также отметить такое направление антивирусных средств, как антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера. Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера. Однако, как и в случае с программными блокировщиками, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS-утилиты FDISK немедленно вызывает «ложное срабатывание» защиты.

Существует несколько более универсальных аппаратных блокировщиков, но к перечисленным выше недостаткам добавляются также проблемы совместимости со стандартными конфигурациями компьютеров и сложности при их установке и настройке. Все это делает аппаратные блокировщики крайне непопулярными на фоне остальных типов антивирусной защиты.

**2.4 Сравнение антивирусных пакетов**

Вне зависимости от того, какую информационную систему нужно защищать, наиболее важный параметр при сравнении антивирусов – способность обнаруживать вирусы и другие вредоносные программы.

Однако этот параметр хотя и важный, но далеко не единственный.

Дело в том, что эффективность системы антивирусной защиты зависит не только от ее способности обнаруживать и нейтрализовать вирусы, но и от множества других факторов.

Антивирус должен быть удобным в работе, не отвлекая пользователя компьютера от выполнения его прямых обязанностей. Если антивирус будет раздражать пользователя настойчивыми просьбами и сообщениями, рано или поздно он будет отключен. Интерфейс антивируса должен быть дружественным и понятным, так как далеко не все пользователи обладают большим опытом работы с компьютерными программами. Не разобравшись со смыслом появившегося на экране сообщения, можно невольно допустить вирусное заражение даже при установленном антивирусе.

Наиболее удобен режим антивирусной защиты, когда проверке подвергаются все открываемые файлы. Если антивирус не способен работать в таком режиме, пользователю придется для обнаружения вновь появившихся вирусов каждый день запускать сканирование всех дисков. На эту процедуру могут уйти десятки минут или даже часы, если речь идет о дисках большого объема, установленных, например, на сервере.

Так как новые вирусы появляются каждый день, необходимо периодически обновлять базу данных антивируса. В противном случае эффективность антивирусной защиты будет очень низкой. Современные антивирусы после соответствующей настройки могут автоматически обновлять антивирусные базы данных через Интернет, не отвлекая пользователей и администраторов на выполнение этой рутинной работы.

При защите крупной корпоративной сети на передний план выдвигается такой параметр сравнения антивирусов, как наличие сетевого центра управления. Если корпоративная сеть объединяет сотни и тысячи рабочих станций, десятки и сотни серверов, то без сетевого центра управления эффективную антивирусную защиту организовать практически невозможно. Один или несколько системных администраторов не смогут обойти все рабочие станции и серверы, установив на них и настроив антивирусные программы. Здесь необходимы технологии, допускающие централизованную установку и настройку антивирусов на все компьютеры корпоративной сети.

Защита узлов Интернета, таких как почтовые серверы, и серверов служб обмена сообщениями требует применения специализированных антивирусных средств. Обычные антивирусы, предназначенные для проверки файлов, не смогут найти вредоносный программный код в базах данных серверов обмена сообщениями или в потоке данных, проходящих через почтовые серверы.

Обычно при сравнении антивирусных средств учитывают и другие факторы. Государственные учреждения могут при прочих равных условиях предпочесть антивирусы отечественного производства, имеющие все необходимые сертификаты. Немалую роль играет и репутация, полученная тем или иным антивирусным средством среди пользователей компьютеров и системных администраторов. Немалую роль при выборе могут играть и личные предпочтения.

Для доказательства преимуществ своих продуктов разработчики антивирусов часто используют результаты независимых тестов. При этом пользователи зачастую не понимают, что конкретно и каким образом проверялось в данном тесте.

В данной работе сравнительному анализу подверглись наиболее популярные на данный момент антивирусные программы, а именно: Антивирус Касперского, Symantec/Norton, Доктор Веб, Eset Nod32, Trend Micro, McAfee, Panda, Sophos, BitDefender, F-Secure, Avira, Avast!, AVG, Microsoft.

Одним из первых тестировать антивирусные продукты начал британский журнал Virus Bulletin. Первые тесты, опубликованные на их сайте, относятся к 1998 году. Основу теста составляет коллекция вредоносных программ WildList. Для успешного прохождения теста необходимо выявить все вирусы этой коллекции и продемонстрировать нулевой уровень ложных срабатываний на коллекции «чистых» файлов журнала. Тестирование проводится несколько раз в год на различных операционных системах; успешно прошедшие тест продукты получают награду VB100%. На рисунке 1 отражено, сколько наград VB100% было получено продуктами различных антивирусных компаний.

Безусловно, журнал Virus Bulletin можно назвать старейшим антивирусным тестером, но статус патриарха не избавляет его от критики антивирусного сообщества. Во-первых, WildList включает в себя только вирусы и черви и только для платформы Windows. Во-вторых, коллекция WildList содержит небольшое число вредоносных программ и очень медленно пополняется: за месяц в коллекции появляется всего несколько десятков новых вирусов, тогда как, например, коллекция AV-Test за это время пополняется несколькими десятками или даже сотнями тысяч экземпляров вредоносного программного обеспечения.

Все это говорит о том, что в настоящем своем виде коллекция WildList морально устарела и не отражает реальной ситуации с вирусами в сети Интернет. В результате тесты, основанные на коллекции WildList, становятся все более бессмысленными. Они хороши для рекламы продуктов, которые их прошли, но реально качество антивирусной защиты они не отражают.

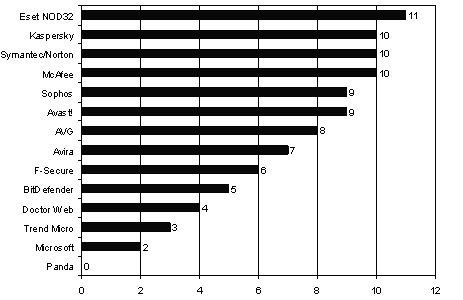


Рисунок 1 – Количество успешно пройденных тестов VB 100%

Независимые исследовательские лаборатории, такие как AV-Comparatives, AV-Tests, дважды в год проводят тестирование антивирусных продуктов на уровень обнаружения вредоносных программ по требованию. При этом коллекции, на которых проводится тестирование, содержат до миллиона вредоносных программ и регулярно обновляются. Результаты тестов публикуются на сайтах этих организаций (www.AV-Comparatives.org, www.AV-Test.org) и в известных компьютерных журналах PC World, PC Welt. Итоги очередных тестов представлены ниже:

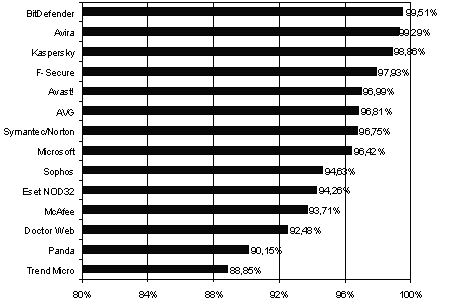


Рисунок 2 – Общий уровень обнаружения вредоносного программного обеспечения по мнению AV-Test

Если говорить о наиболее распространенных продуктах, то по результатам этих тестов в тройку лидеров входят только решения Лаборатории Касперского и Symantec. Отдельного внимания заслуживает лидирующая в тестах Avira.

Тесты исследовательских лабораторий AV-Comparatives и AV-Test, так же как и любые тесты, имеют свои плюсы и свои минусы. Плюсы заключаются в том, что тестирование проводится на больших коллекциях вредоносного программного обеспечения, и в том, что в этих коллекциях представлены самые разнообразные типы вредоносных программ. Минусы же в том, что в этих коллекциях содержатся не только «свежие» образцы вредоносных программ, но и относительно старые. Как правило, используются образцы, собранные за последние полгода. Кроме того, в ходе этих тестов анализируются результаты проверки жесткого диска по требованию, тогда как в реальной жизни пользователь скачивает заражённые файлы из Интернета или получает их в виде вложений по электронной почте. Важно обнаруживать такие файлы именно в момент появления их на компьютере пользователя.

Попытку выработать методику тестирования, не страдающую от этой проблемы, предпринял один из старейших британских компьютерных журналов – PC Pro. В их тесте использовалась коллекция вредоносных программ, обнаруженных за две недели до проведения теста в трафике, проходящем через серверы компании MessageLabs. MessageLabs предлагает своим клиентам сервисы по фильтрации различных видов трафика, и ее коллекция вредоносных программ реально отражает ситуацию с распространением компьютерных вирусов в Сети.

Команда журнала PC Pro не просто сканировала зараженные файлы, а моделировала действия пользователя: зараженные файлы прикреплялись к письмам в виде вложений и эти письма скачивались на компьютер с установленным антивирусом. Кроме того, при помощи специально написанных скриптов зараженные файлы скачивались с Web-сервера, то есть моделировался серфинг пользователя в Интернете. Условия, в которых проводятся подобные тесты, максимально приближены к реальным, что не могло не отразится на результатах: уровень обнаружения у большинства антивирусов оказался существенно ниже, чем при простой проверке по требованию в тестах AV-Comparatives и AV-Test. В таких тестах немаловажную роль играет то, насколько быстро разработчики антивируса реагируют на появление новых вредоносных программ, а также какие проактивные механизмы используются при обнаружении вредоносных программ.

Скорость выпуска обновлений антивируса с сигнатурами новых вредоносных программ – это одна из самых важных составляющих эффективной антивирусной защиты. Чем быстрее будет выпущено обновление баз сигнатур, тем меньшее время пользователь останется незащищенным.

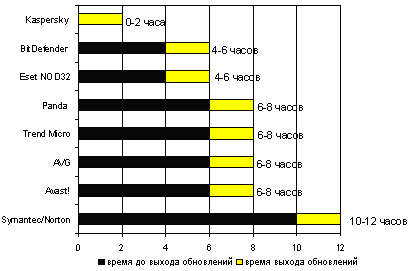


Рисунок 3 – Среднее время реакции на новые угрозы

В последнее время новые вредоносные программы появляются так часто, что антивирусные лаборатории едва успевают реагировать на появление новых образцов. В подобной ситуации встает вопрос о том, как антивирус может противостоять не только уже известным вирусам, но и новым угрозам, для обнаружения которых еще не выпущена сигнатура.

Для обнаружения неизвестных угроз используются так называемые проактивные технологии. Можно разделить эти технологии на два вида: эвристики (обнаруживают вредоносные программы на основе анализа их кода) и поведенческие блокираторы (блокируют действия вредоносных программ при их запуске на компьютере, основываясь на их поведении).

Если говорить об эвристиках, то их эффективность уже давно изучает AV-Comparatives – исследовательская лаборатория под руководством Андреаса Клименти. Команда AV-Comparatives применяет особую методику: антивирусы проверяются на актуальной вирусной коллекции, но при этом используется антивирус с сигнатурами трехмесячной давности. Таким образом, антивирусу приходится противостоять вредоносным программам, о которых он ничего не знает. Антивирусы проверяются путем сканирования коллекции вредоносного программного обеспечения на жестком диске, поэтому проверяется только эффективность эвристика. Другая проактивная технология – поведенческий блокиратор – в этих тестах не задействуется. Даже самые лучшие эвристики на данный момент показывают уровень обнаружения только около 70%, а многие из них еще и болеют ложными срабатываниями на чистых файлах. Все это говорит о том, что пока этот проактивный метод обнаружения может использоваться только одновременно с сигнатурным методом.

Что же касается другой проактивной технологии – поведенческого блокиратора, то в этой области серьезных сравнительных тестов не проводилось. Во-первых, во многих антивирусных продуктах («Доктор Веб», NOD32, Avira и других) отсутствует поведенческий блокиратор. Во-вторых, проведение таких тестов сопряжено с некоторыми трудностями. Дело в том, что для проверки эффективности поведенческого блокиратора необходимо не сканировать диск с коллекцией вредоносных программ, а запускать эти программы на компьютере и наблюдать, насколько успешно антивирус блокирует их действия. Этот процесс очень трудоемкий, и лишь немногие исследователи способны взяться за проведение таких тестов. Все, что пока доступно широкой общественности, это результаты тестирования отдельных продуктов, проведенного командой AV-Comparatives. Если в ходе тестирования антивирусы успешно блокировали действия неизвестных им вредоносных программ во время их запуска на компьютере, то продукт получал награду Proactive Protection Award. В настоящий момент такие награды получили F-Secure c поведенческой технологией DeepGuard и «Антивирус Касперского» с модулем «Проактивная защита».

Технологии предупреждения заражения, основанные на анализе поведения вредоносных программ, получают все большее распространение, и отсутствие комплексных сравнительных тестов в этой области не может не тревожить. Недавно специалисты исследовательской лаборатории AV-Test провели широкое обсуждение этого вопроса, в котором участвовали и разработчики антивирусных продуктов. Итогом этого обсуждения явилась новая методика тестирования способности антивирусных продуктов противостоять неизвестным угрозам.

Высокий уровень обнаружения вредоносных программ при помощи различных технологий является одной из важнейших характеристик антивируса. Однако не менее важной характеристикой является отсутствие ложных срабатываний. Ложные срабатывания могут нанести не меньший вред пользователю, чем вирусное заражение: заблокировать работу нужных программ, перекрыть доступ к сайтам и так далее.

В ходе своих исследований AV-Comparatives, наряду с изучением возможностей антивирусов по обнаружению вредоносного ПО, проводит и тесты на ложные срабатывания на коллекциях чистых файлов. Согласно тесту наибольшее количество ложных срабатываний обнаружено у антивирусов «Доктор Веб» и Avira.

Стопроцентной защиты от вирусов не существует. Пользователи время от времени сталкиваются с ситуацией, когда вредоносная программа проникла на компьютер и компьютер оказался заражен. Это происходит либо потому, что на компьютере вообще не было антивируса, либо потому, что антивирус не обнаружил вредоносную программу ни сигнатурными, ни проактивными методами. В такой ситуации важно, чтобы при установке антивируса со свежими базами сигнатур на компьютере антивирус смог не только обнаружить вредоносную программу, но и успешно ликвидировать все последствия ее деятельности, вылечить активное заражение. При этом важно понимать, что создатели вирусов постоянно совершенствуют свое «мастерство», и некоторые их творения достаточно трудно удалить с компьютера – вредоносные программы могут разными способами маскировать свое присутствие в системе (в том числе при помощи руткитов) и даже противодействовать работе антивирусных программ. Кроме того, не достаточно просто удалить или вылечить зараженный файл, нужно ликвидировать все изменения, произведенные вредоносным процессом в системе и полностью восстановить работоспособность системы. Команда российского портала Anti-Malware.ru провели подобный тест, его результаты представлены на рисунке 4.

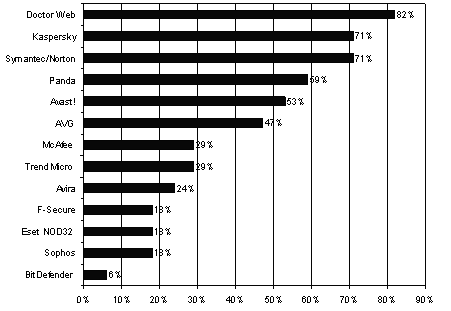


Рисунок 4 – Лечение активного заражения

Выше были рассмотрены различные подходы к тестированию антивирусов, показано, какие параметры работы антивирусов рассматриваются при тестировании. Можно сделать вывод, что у одних антивирусов выигрышным оказывается один показатель, у других – другой. При этом естественно, что в своих рекламных материалах разработчики антивирусов делают упор только на те тесты, где их продукты занимают лидирующие позиции. Так, например, «Лаборатория Касперского» делает акцент на скорости реакции на появление новых угроз, Еset – на силе своих эвристических технологий, «Доктор Веб» описывает свои преимущества в лечении активного заражения.

Таким образом, следует провести синтез результатов различных тестов. Так сведены позиции, которые антивирусы заняли в рассмотренных тестах, а также выведена интегрированная оценка – какое место в среднем по всем тестам занимает тот или иной продукт. В итоге в тройке призеров: «Касперский», Avira, Symantec.

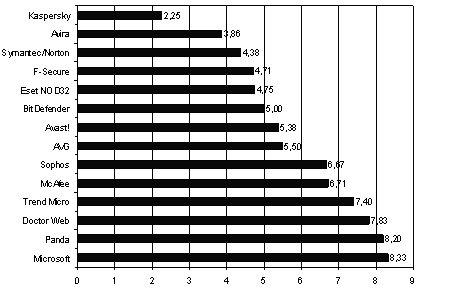


Рисунок 5 – Усредненный рейтинг антивирусных программ

На основе проанализированных антивирусных пакетов был создан программный продукт, предназначенный для поиска и лечения файлов, зараженных вирусом SVC 5.0. Данный вирус на приводит к несанкционированному удалению или копированию файлов, однако значительно мешает полноценной работе с программным обеспечением компьютера.

Зараженные программы имеют длину большую, чем исходный код. Однако при просмотре каталогов на зараженной машине этого видно не будет, так как вирус проверяет, заражен найденный файл или нет. Если файл заражен, то в DTA записывается длина незараженного файла.

Обнаружить данный вирус можно следующим образом. В области данных вируса есть символьная строка "(c) 1990 by SVC,Ver. 5.0", по которой вирус, если он есть на диске, можно обнаружить.

При написании антивирусной программы выполняется следующая последовательность действий:

1 Для каждого проверяемого файла определяется время его создания.

2 Если число секунд равно шестидесяти, то проверяются три байта по смещению, равному "длина файла минус 8АН". Если они равны соответственно 35Н, 2ЕН, 30Н, то файл заражен.

3 Выполняется декодирование первых 24 байт оригинального кода, которые расположены по смещению "длина файла минус 01CFН плюс 0BAAН". Ключи для декодирования расположены по смещению "длина файла минус 01CFН плюс 0С1AН" и "длина файла минус 01CFН плюс 0С1BН".

4 Раскодированные байты переписываются в начало программы.

5 Файл «усекается» до величины "длина файла минус 0С1F".

Программа создана в среде программирования Turbo Pascal. Текст программы изложен в Приложении А.

**Заключение**

В данной курсовой работе был проведен сравнительный анализ антивирусных пакетов.

В процессе проведения анализа были успешно решены задачи, поставленные в начале работы. Так были изучены понятия информационной безопасности, компьютерных вирусов и антивирусных средств, определены виды угроз безопасности информации, методы защиты, рассмотрена классификация компьютерных вирусов и антивирусных программ и проведен сравнительный анализ антивирусных пакетов, написана программа, производящая поиск зараженных файлов.

Результаты, полученные в процессе работы могут быть применены при выборе антивирусного средства.

Все полученные результаты отражены в работе с помощью диаграмм, поэтому пользователь может самостоятельно проверить выводы, сделанные в итоговой диаграмме, отражающей синтез выявленных результатов различных тестов антивирусных средств.

Результаты, полученные в процессе работы могут быть применены как основа для самостоятельного сравнения антивирусных программ.

В свете широкого использования IT-технологий, представленная курсовая работа является актуальной и отвечает предъявленным к ней требованиям. В процессе работы были рассмотрены наиболее популярные антивирусные средства.

**Список использованной литературы**

1 Анин Б. Защита компьютерной информации. – СПб. : БХВ – Санкт – Петербург, 2000. – 368 с.

2 Артюнов В. В. Защита информации: учеб. – метод. пособие. М. : Либерия – Бибинформ, 2008. – 55 с. – (Библиотекарь и время. 21 век; вып. №99 ).

3 Корнеев И. К., Е. А. Степанов Защита информации в офисе: учебник. – М . : Проспект, 2008. – 333 с.

5 Куприянов А. И. Основы защиты информации: учеб. пособие. – 2-е изд. стер. – М.: Академия, 2007. – 254 с. – (Высшее профессиональное образование).

6 Семененко В. А., Н. В. Федоров Программно – аппаратная защита информации: учеб. пособие для студ. вузов. – М. : МГИУ, 2007. – 340 с.

7 Цирлов В. Л. Основы информационной безопасности: краткий курс. – Ростов н/Д: Феникс, 2008. – 254 с. (Профессиональное образование).

**Приложение**

**Листинг программы**

Program ANTIVIRUS;

Uses dos,crt,printer;

Type St80 = String[80];

Var

R:Registers;

FileInfection:File Of Byte;

SearchFile:SearchRec;

Mas:Array[0..80] of St80;

MasByte:Array[1..3] of Byte;

Position,I,J,K:Byte;

Num,NumberOfFile,NumberOfInfFile:Word;

St:St80;

Flag,NextDisk,Error:Boolean;

Dt:DateTime;

Key1,Key2,Key3,NumError:Byte;

MasScreen:Array[0..24,0..159] Of Byte Absolute $B800:0000;

Ch,Disk:Char;

Procedure Cure(St : St80);

Var

I: Byte; MasCure: Array[1..24] Of Byte;

Begin

Assign(FileInfection,St); Reset(FileInfection);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Seek(FileInfection,FileSize(FileInfection) - ($0C1F - $0C1A));

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Read(FileInfection,Key1);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Read(FileInfection,Key2);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Seek(FileInfection,FileSize(FileInfection) - ($0C1F - $0BAA));

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

For I:=1 to 24 do

Begin

Read(FileInfection,MasCure[i]);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Key3:=MasCure[i];

InLine($50/

$8A/$26/KEY1/

$30/$26/KEY3/

$A0/KEY2/

$00/$C4/

$88/$26/KEY1/

$58);

MasCure[i]:=Key3;

End;

Seek(FileInfection,0);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

For I:=1 to 24 do Write(FileInfection,MasCure[i]);

Seek(FileInfection,FileSize(FileInfection) - $0C1F);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Truncate(FileInfection);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Close(FileInfection); NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Num:=Num+1;

End;

Procedure F1(St : St80);

Begin

FindFirst(St + '\*.\*', $3F, SearchFile);

While (SearchFile.Attr = $10) And (DosError = 0) And

((SearchFile.Name = '.') Or (SearchFile.Name = '..')) Do

Begin

FindNext(SearchFile);

End;

While (DosError = 0) Do

Begin

If KeyPressed Then

If (Ord(ReadKey) = 27) Then Halt;

If (SearchFile.Attr = $10) Then

Begin

Mas[k]:=St + SearchFile.Name + '\';

K:=K+1;

End;

If (SearchFile.Attr <> $10) Then

Begin

NumberOfFile:=NumberOfFile + 1;

UnpackTime(SearchFile.Time, DT);

For I:=18 to 70 do MasScreen[6,2\*i]:=$20;

GoToXY(18,7);

Write(St + SearchFile.Name,' ');

If (Dt.Sec = 60) Then

Begin

Assign(FileInfection,St + SearchFile.Name);

Reset(FileInfection);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

Seek(FileInfection,FileSize(FileInfection) - $8A);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

For I:=1 to 3 do Read(FileInfection,MasByte[i]);

Close(FileInfection);

NumError:=IOResult;

If (NumError <> 0) Then Begin Error:=True; Exit; End;

If (MasByte[1] = $35) And (MasByte[2] = $2E) And

(MasByte[3] = $30) Then

Begin

NumberOfInfFile:=NumberOfInfFile + 1;

GoToXY(1,8);

Write( St + SearchFile.Name,' inficirovan. ',

'Udalit? [Y/N] ');

Repeat

Ch:=ReadKey;

If (Ord(Ch) = 27) Then Exit;

Until (Ch = 'Y') Or (Ch = 'y') Or (Ch = 'N')

Or (Ch = 'n');

If (Ch = 'Y') Or (Ch = 'y') Then

Begin

Cure(St + SearchFile.Name);

If (NumError <> 0) Then Exit;

End;

For I:=0 to 79 do MasScreen[7,2\*i]:=$20;

End; End; End;

FindNext(SearchFile);

End;

End;

Begin

Repeat

Flag:=True;

TextAttr:=$1F;

Repeat

ClrScr;

GoToXY(29,1); TextAttr:=$1E; GoToXY(20,2); TextAttr:=$17;

Writeln('Programma dlya poiska i lecheniya fajlov,');

GoToXY(28,3);

Writeln('zaragennih SVC50.');

TextAttr:=$4F; GoToXY(1,25);

Write(' ESC - exit ');

TextAttr:=$1F; GoToXY(1,6);

Write('Kakoj disk proverit? ');

Disk:=ReadKey;

If (Ord(Disk) = 27) Then Exit;

R.Ah:=$0E; R.Dl:=Ord(UpCase(Disk))-65;

Intr($21,R); R.Ah:=$19; Intr($21,R);

Flag:=(R.Al = (Ord(UpCase(Disk))-65));

Until Flag;

NextDisk:=True;

Error:=False;

Num:=0;

K:=0;

St:=UpCase(Disk) + ':\';

GoToXY(1,6);

Writeln('Testiruetsya disk ',St,' ');

Writeln('Testiruetsya fajl ');

NumberOfFile:=0;

NumberOfInfFile:=0;

F1(St);

If (k = 0) Or Error Then Flag:=False;

If (k > 0) Then K:=K-1;

While Flag Do

Begin

If (k=0) Then Flag:=False;

F1(Mas[k]);

If (k > 0) Then K:=K-1;

End;

GoToXY(1,10);

Writeln('Provereno fajlov - ',NumberOfFile);

Writeln('Zarageno fajlov - ',NumberOfInfFile);

Writeln('Izlecheno fajlov - ',Num);

Write('Proverit drugoj disk? [Y/N]');

Repeat

Ch:=ReadKey;

If (Ord(Ch) = 27) Then Exit;

Until (Ch = 'Y') Or (Ch = 'y') Or (Ch = 'N') Or (Ch = 'n');

If (Ch = 'N') Or (Ch = 'n') Then NextDisk:=False;

Until Not(NextDisk);

End.