**ВПО – вредоносное программное обеспечение**

**Введение**

К концу двадцатого века люди овладели многими тайнами превращения вещества и энергии и сумели использовать эти знания для улучшения своей жизни. Но кроме вещества и энергии в жизни человека огромную роль играет еще одна составляющая - информация. Это самые разнообразные сведения, сообщения, известия, знания, умения. В середине нашего столетия появились специальные устройства - компьютеры, ориентированные на хранение и преобразование информации и произошла компьютерная революция. В связи со стремительным развитием информационных технологий и их проникновением во все сферы человеческой деятельности возросло количество преступлений, направленных против информационной безопасности. Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным 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, казалось бы, идентичных продуктов. Их пользователи, представляя проблему лишь в общих чертах, нередко упускают важные нюансы и в итоге получают иллюзию защиты вместо самой защиты.

**1. Понятие - ВПО.**

**Вредоносная программа** - *программа*, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. Иными словами вредоносной программой называют некоторый самостоятельный набор инструкций, который способен выполнять следующее:

1. скрывать свое присутствие в компьютере;
2. обладать способностью к самоуничтожению, маскировкой под легальные программы и копирования себя в другие области оперативной или внешней памяти;
3. модифицировать (разрушать, искажать) код других программ;
4. самостоятельно выполнять деструктивные функции - копирование, модификацию, уничтожение, блокирование и т.п.
5. искажать, блокировать или подменять выводимую во внешний канал связи или на внешний носитель информацию.

Основными путями проникновения вредоносных программ в *АС*, в частности, на *компьютер*, являются сетевое взаимодействие и съемные носители информации (флешки, диски и т.п.). При этом внедрение в систему может носить случайный характер.

**Основными видами вредоносных программ** являются:

* программные закладки;
* программные вирусы;
* сетевые черви;
* другие вредоносные программы, предназначенные для осуществления НСД.

**1.2. Программные закладки**

К **программным закладкам** относятся программы и фрагменты программного кода, предназначенные для формирования недекларированных возможностей легального программного обеспечения.

**Недекларированные возможности программного обеспечения** - функциональные возможности программного обеспечения, не описанные в документации. Программная закладка часто служит проводником для других вирусов и, как правило, не обнаруживаются стандартными средствами антивирусного контроля.

Закладки иногда делят на **программные и аппаратные**, но фактически все закладки - программные, так как под аппаратными закладками подразумеваются так называемые прошивки.

Программные закладки различают в **зависимости от метода их внедрения в систему:**

* программно-аппаратные. Это закладки, интегрированные в программно-аппаратные средства ПК (BIOS, прошивки периферийного оборудования);
* загрузочные. Это закладки, интегрированные в программы начальной загрузки (программы-загрузчики), располагающиеся в загрузочных секторах;
* драйверные. Это закладки, интегрированные в драйверы (файлами, необходимые операционной системе для управления подключенными к компьютеру периферийными устройствами);
* прикладные. Это закладки, интегрированные в прикладное программное обеспечение (текстовые редакторы, графические редакторы, различные утилиты и т.п.);
* исполняемые. Это закладки, интегрированные в исполняемые программные модули. Программные модули чаще всего представляют собой пакетные файлы, которые состоят из команд операционной системы, выполняемых одна за другой, как если бы их набирали на клавиатуре компьютера;
* закладки-имитаторы. Это закладки, которые с помощью похожего интерфейса имитируют программы, в ходе работы которых требуется вводить конфиденциальную информацию;

Для выявления программных закладок часто используется **качественный подход**, заключающийся в наблюдении за функционированием системы, а именно:

1. снижение быстродействия;
2. изменение состава и длины файлов;
3. частичное или полное блокирование работы системы и ее компонентов;
4. имитация физических (аппаратных) сбоев работы вычислительных средств и периферийных устройств;
5. переадресация сообщений;
6. обход программно-аппаратных средств криптографического преобразования информации;
7. обеспечение доступа в систему с несанкционированных устройств.

Существуют также диагностические методы обнаружения закладок. Так, например, антивирусы успешно находят загрузочные закладки. С инициированием статической ошибки на дисках хорошо справляется *Disk* Doctor, входящий в распространенный комплекс утилит Norton Utilities. К наиболее распространенным программным закладкам относится "*троянский конь*".

**Троянским конем** называется:

* программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба;
* программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия.

Перечислим **основные виды троянских программ и их возможности**:

* Trojan-Notifier - Оповещение об успешной атаке. Троянцы данного типа предназначены для сообщения своему "хозяину" о зараженном компьютере. При этом на адрес "хозяина" отправляется информация о компьютере, например, IP-адрес компьютера, номер открытого порта, адрес электронной почты и т. п.
* Trojan-PSW - Воровство паролей. Они похищают конфиденциальные данные с компьютера и передают их хозяину по электронной почте.
* Trojan-Clicker - интернет-кликеры - Семейство троянских программ, основная функция которых - организация несанкционированных обращений к интернет-ресурсам (обычно к веб-страницам). Методы для этого используются разные, например установка злонамеренной страницы в качестве домашней в браузере.
* Trojan-DDoS - Trojan-DDoS превращают зараженный компьютер в так называемый бот, который используется для организации атак отказа в доступе на определенный сайт. Далее от владельца сайта требуют заплатить деньги за прекращение атаки.
* Trojan-Proxy - Троянские прокси-сервера. Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным Интернет-ресурсам. Обычно используются для рассылки спама.
* Trojan-Spy - Шпионские программы. Они способны отслеживать все ваши действия на зараженном компьютере и передавать данные своему хозяину. В число этих данных могут попасть пароли, аудио и видео файлы с микрофона и видеокамеры, подключенных к компьютеру.
* Backdoor - Способны выполнять удаленное управление зараженным компьютером. Его возможности безграничны, весь ваш компьютер будет в распоряжении хозяина программы. Он сможет рассылать от вашего имени сообщения, знакомиться со всей информацией на компьютере, или просто разрушить систему и данные без вашего ведома.
* Trojan-Dropper - Инсталляторы прочих вредоносных программ. Очень похожи на Trojan-Downloader, но они устанавливают злонамеренные программы, которые содержатся в них самих.
* Rootkit - способны прятаться в системе путем подмены собой различных объектов. Такие трояны весьма неприятны, поскольку способны заменить своим программным кодом исходный код операционной системы, что не дает антивирусу возможности выявить наличие вируса.

**1.3. Компьютерные вирусы и сетевые черви**

**Вирусы** - вредоносные программы, которые несанкционированно многократно копирует свой код, присоединяя его к кодам других программ («размножается») и мешает корректной работе компьютера и/или разрушает хранимую на магнитных дисках информацию (программы и данные).

Существуют вирусы и менее «злокачественные», вызывающие, например, переустановку даты в компьютере, музыкальные (проигрывающие какую-либо мелодию), приводящие к появлению на экране дисплея какого-либо изображения или к искажениям в отображении дисплеем информации, «осыпанию букв» и т.д.

Создание компьютерных вирусов можно квалифицировать с юридической точки зрения как преступление.

**Жизненный цикл** вируса состоит из следующих этапов:

* Проникновение на компьютер
* Активация вируса
* Поиск объектов для заражения
* Подготовка вирусных копий
* Внедрение вирусных копий

Основные **деструктивные действия**, выполняемые вирусами и червями:

1. перезагрузка каналов связи
2. атаки "отказ в обслуживании"
3. потеря данных
4. нарушение работы ПО
5. загрузка ресурсов компьютера
6. хищение информации.

Вирусы классифицируют по **местам заражения и местам нахождения следов вредоносной деятельности.**

* *Вирусы-спутники* исполняемых файлов с расширением \*.ехе. Создается одноименная копия \*.соm вируса, которая из-за особенностей операционной системы всегда запускается раньше, чем основной \*.ехе файл.
* *Файловые вирусы.* Поражают все виды двоичных исполняемых файлов, драйверы, объектные модули и системные библиотеки, записывая свое тело внутрь исполняемой программы таким образом, чтобы при запуске зараженной программы первоначально "приступал к работе" вирус.
* *Загрузочные вирусы.* Записывают в загрузочные сектора носителей информации головку вируса, размещая тело (большую часть кода) внутри отдельных файлов или программ, почти как файловые вирусы. Загрузочные сектора носителей читаются всегда при обращении к носителю, это позволяет активизировать вирус без открытия файла при вызове окна диска, выводе списка файлов, просмотре структуры дерева каталогов.
* *Dir-вирусы* (от слова директорий – каталог). Размещают свою "головку" таким образом, чтобы активизироваться при просмотре зараженного каталога или структуры дерева каталогов.
* *Макровирусы.* Способны проникать и заражать неисполняемые файлы, например файлы с документами и шаблонами, подготовленные с помощью текстового редактора Word, табличного процессора Excel. Переносятся и копируются вместе с зараженными документами.

Следует упомянуть **сетевые вирусы**, распространяющиеся в сетях, объединяющих многие десятки и сотни тысяч компьютеров.

Рассмотрим **принципы функционирования загрузочных вирусов**. На каждой дискете или винчестере имеются служебные сектора, используемые операционной системой для собственных нужд, в том числе сектор начальной загрузки. В нем помимо информации о дискете (число дорожек, число секторов и пр.) хранится небольшая программа начальной загрузки.

Простейшие загрузочные вирусы, резидентно находясь в памяти зараженного компьютера, обнаруживают в дисководе незараженную дискету и производят **следующие действия**:

* выделяют некоторую область дискеты и делают ее недоступной операционной системе (помечая, например, как сбойную - bad);
* замещают программу начальной загрузки в загрузочном секторе дискеты, копируя корректную программу загрузки, а также свой код, в выделенную область дискеты;
* организуют передачу управления так, чтобы вначале выполнялся бы код вируса и лишь затем - программа начальной загрузки.

Теперь рассмотрим принципы функционирования **файловых вирусов**. Файловый вирус не обязательно является резидентным, он может, например, внедриться в код исполняемого файла. При запуске зараженного файла вирус получает управление, выполняет некоторые действия и возвращает управление коду, в который он был внедрен. Действия, которые выполняет вирус, включает поиск подходящего для заражения файла, внедрение в него так, чтобы получить управление файла, произведение некоторого эффекта, например, звукового или графического. Если файловый вирус резидентный, то он устанавливается в памяти и получает возможность заражать файлы и проявляться независимо от первоначального зараженного файла.

**Файловые вирусы** - вирусы, которые заражают непосредственно файлы. Файловые вирусы можно разделить на три группы в зависимости от среды, в которой распространяется *вирус*:

1. **Файловые вирусы** - работают непосредственно с ресурсами операционной системы. Пример: один из самых известных вирусов получил название "Чернобыль". Благодаря своему небольшому размеру (1 Кб) вирус заражал PE-файлы таким образом, что их размер не менялся. Для достижения этого эффекта вирус ищет в файлах "пустые" участки, возникающие из-за выравнивания начала каждой секции файла под кратные значения байт. После получения управления вирус перехватывает IFS API, отслеживая вызовы функции обращения к файлам и заражая исполняемые файлы. 26 апреля срабатывает деструктивная функция вируса, которая заключается в стирании Flash BIOS и начальных секторов жестких дисков. Результатом является неспособность компьютера загружаться вообще (в случае успешной попытки стереть Flash BIOS) либо потеря данных на всех жестких дисках компьютера.
2. **Макровирусы** - вирусы, написанные на макроязыках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.п.). Самыми распространенными являются вирусы для программ Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя (свои копии) из одного документа в другой.

Для существования макровирсуов в конкретном редакторе встроенный в него макроязык должен обладать следующими возможностями:

* 1. привязка программы на макроязыке к конкретному файлу;
  2. копирование макропрограмм из одного файла в другой;
  3. получение управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

1. **Сетевые вирусы** - вирусы, которые для своего распространения используют протоколы и возможности локальных и глобальных сетей. Основным свойством сетевого вируса является возможность самостоятельно тиражировать себя по сети. При этом существуют сетевые вирусы, способные запустить себя на удаленной станции или сервере.

Заражая файл, вирус всегда изменит его код, но далеко не всегда производит другие изменения. В частности, может не изменяться начало файла и его длина (что раньше считалось признаком заражения). Например, вирусы могут искажать информацию о файлах, хранящуюся в служебной области магнитных дисков - таблице размещения файлов (Fat - file allocation table), - делать таким образом невозможным любую работу с файлами. Так ведут себя вирусы **семейства «Dir».**

*Загрузочно-файловые вирусы* используют принципы как загрузочных, так и файловых вирусов, и являются наиболее опасными.

**Червь** (*сетевой червь*) - тип вредоносных программ, распространяющихся *по* сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

Можно заметить схожесть сетевых червей и компьютерных вирусов, в частности, полное совпадение жизненного *цикла* и самотиражирование. Основным отличием червей от программных вирусов является способность к распространению *по* сети без участия человека. Иногда сетевых червей относят к подклассу компьютерных вирусов.

Самым знаменитым червем является червь Moriss, *механизмы* работы которого подробно описаны в литературе. Червь появился в 1988 году и в течение короткого промежутка времени парализовал работу многих компьютеров в Интернете. Данный червь является "классикой" вредоносных программ, а *механизмы* нападения, разработанные автором при его написании, до сих пор используются злоумышленниками. Moriss являлся самораспространяющейся программой, которая распространяла свои копии *по* сети, получая привилегированные *права* доступа на хостах сети за счет использования уязвимостей в операционной системе. Одной из уязвимостей, использованных червем, была уязвимая версия программы sendmail (*функция* "*debug*" программы sendmail, которая устанавливала отладочный режим для текущего сеанса связи), а другой - *программа* fingerd (в ней содержалась ошибка переполнения буфера). Для поражения систем червь использовал также *уязвимость* команд rexec и rsh, а также неверно выбранные пользовательские пароли.

На этапе проникновения в систему черви делятся преимущественно **по типам используемых протоколов**:

* Сетевые черви - черви, использующие для распространения протоколы Интернет и локальных сетей. Обычно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов tcp/ip
* Почтовые черви - черви, распространяющиеся в формате сообщений электронной почты. Как правило, в письме содержится тело кода или ссылка на зараженный ресурс. Когда вы запускаете прикрепленный файл, червь активизируется; когда вы щелкаете на ссылке, загружаете, а затем открываете файл, червь также начинает выполнять свое вредоносное действие. После этого он продолжает распространять свои копии, разыскивая другие электронные адреса и отправляя по ним зараженные сообщения. Для отправки сообщений червями используются следующие способы: прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку; использование сервисов MS Outlook; использование функций Windows MAPI.Встречаются экземпляры, которые могут комбинировать способы.
* IRC-черви - черви, распространяющиеся по каналам IRC (Internet Relay Chat). Черви этого класса используют два вида распространения: посылание пользователю URL-ссылки на файл-тело; отсылку пользователю файла (при этом пользователь должен подтвердить прием).
* P2P-черви - черви, распространяющиеся при помощи пиринговых (peer-to-peer) файлообменных сетей. Механизм работы большинства подобных червей достаточно прост: для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по его распространению P2P-сеть берет на себя - при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для его скачивания с зараженного компьютера. Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и положительно отвечают на поисковые запросы (при этом червь предлагает для скачивания свою копию).
* IM-черви - черви, использующие для распространения системы мгновенного обмена сообщениями (IM, Instant Messenger - ICQ, MSN Messenger, AIM и др.). Известные компьютерные черви данного типа используют единственный способ распространения - рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL на файл, расположенный на каком-либо веб - сервере. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

Мы перечислили **наиболее распространенные категории сетевых червей**, на практике их значительно больше. Например, в настоящее время всё большую "популярность" приобретают **мобильные черви и черви, распространяющие свои копии через общие сетевые ресурсы**. Последние используют функции операционной системы, в частности, перебирают доступные сетевые папки, подключаются к компьютерам в глобальной сети и пытаются открыть их диски на полный *доступ*. Отличаются от стандартных сетевых червей тем, что пользователю нужно открыть *файл* с копией червя, чтобы активизировать его.

**По деструктивным возможностям вирусы и****сетевые черви** можно разделить на:

* безвредные, т. е. 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 их работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

Но даже если в алгоритме вируса не найдено ветвей, наносящих *ущерб* системе, этот *вирус* нельзя с полной уверенностью назвать безвредным, так как проникновение его в *компьютер* может вызвать непредсказуемые и порой катастрофические последствия. Ведь *вирус*, как и всякая *программа*, имеет ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков (например, вполне безобидный на первый взгляд *вирус* DenZuk довольно корректно работает с 360-килобайтовыми дискетами, но может уничтожить информацию на дискетах большего объема). До сих пор попадаются вирусы, определяющие СОМ или ЕХЕ не *по* внутреннему формату файла, а *по* его расширению. Естественно, что при несовпадении формата и расширения имени *файл* после заражения оказывается неработоспособным. Возможно также "заклинивание" резидентного вируса и системы при использовании новых версий *DOS*, при работе в *Windows* или с другими мощными программными системами. И так далее.

**1.4. Другие вредоносные программы, предназначенные для осуществления НСД.**

Нежелательное программное обеспечение, не несущее непосредственной угрозы для компьютерных систем, но выполняющее непредусмотренные и, как правило, нежелательные для пользователя действия. Такими действиями может быть использование ресурсов компьютерной системы в чужих интересах, вывод на экран монитора рекламной информации (например, в виде всплывающих окон) и иные действия.

К **нежелательному программному обеспечению** относятся:

1) программы-«кликеры» (сlicker), формирующие поток обращений к интернет-ресурсам и тем самым увеличивающие число их посещений;

2) программы-«адвертайзеры» (аdvertizer), показывающие рекламу товаров или услуг;

3) программы-«диалеры» (dialer), предлагающие посетить какой- либо платный ресурс, как правило, порно-сайт;

4) программы-«шутки», сообщающие пользователю об осуществлении нежелательных для него действий (например, об уничтожении данных), которые в действительности не происходят.

**Рискованное программное обеспечение** – легальное программное обеспечение, используемое в злоумышленных целях:

1) утилиты удаленного администрирования;

2) утилиты предоставления сетевого сервиса – proxy-серверы, FTP- серверы и т. д.;

3) утилиты работы с сетевыми ресурсами.

**2. Пути проникновения вируса в компьютер**

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление. Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов.  
Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы. После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И, наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом, заразится все программное обеспечение.

**2.1 Признаки появления вируса**

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие: прекращение работы или неправильная работа ранее успешно функционировавших программ

* медленная работа компьютера
* исчезновение файлов и каталогов или искажение их содержимого
* изменение даты и времени модификации файлов
* изменение размеров файлов
* неожиданное значительное увеличение количества файлов на диске
* существенное уменьшение размера свободной оперативной памяти
* вывод на экран непредусмотренных сообщений или изображений
* подача непредусмотренных звуковых сигналов
* частые зависания и сбои в работе компьютера

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

**2.2 Антивирусные средства**

К настоящему времени накоплен значительный опыт борьбы с компьютерными вирусами, разработаны антивирусные программы, известны меры защиты программ и данных. Происходит постоянное совершенствование, развитие антивирусных средств, которые в короткий срок с момента обнаружения вируса - от недели до месяца - оказываются способными справиться с вновь появляющимися вирусами.

Создание антивирусных программ начинается с обнаружения вируса по аномалиям в работе компьютера. После этого вирус тщательно изучается, выделяется его сигнатура - последовательность байтов, которая полностью характеризует программу вируса (наиболее важные и характерные участки кода), выясняется механизм работы вируса, способы заражения. Полученная информация позволяет разработать способы обнаружения вируса в памяти компьютера и на магнитных дисках, а также алгоритмы обезвреживания вируса (если возможно, удаления вирусного кода из файлов - «лечения»).

**В зависимости от принципа действия** антивирусные программы можно разделить на несколько типов:

1. **Сторожа.** Не выявляют вредоносных программ и тем более не проводят лечения. Сторожа контролируют выполнение некоторых операций на диске, которые часто используют вредоносные программы, и сообщают пользователю об этих операциях. Перечень операций, какая программа и когда их "заставила" выполняться, записывается в журнал. Проанализировав записи в журнале, пользователь может сделать вывод о несанкционированности некоторых операций, о возможном воздействии вредоносных программ.

2. **Детекторы (сканеры).** Программы, содержащие внутри себя или в отдельных подключаемых библиотеках базы данных с цепочками кодов (сигнатурами), присущими ранее выявленным вирусам. Проверяя файлы на наличие таких цепочек, детекторы находят и, вырезая вредоносный код, убивают вирусы. Недостаток детекторов – невозможность обнаружения и лечения новых, незнакомых вирусов, вирусов-невидимок (стеле) и самомодифицирующихся (полиморфных) вирусов. Сканеры, реализующие детектирующие функции, встроены во все современные антивирусные программы.

3. **Полиморфные детекторы**. Программы, создающие на основе одной сигнатуры полиморфного вируса базу данных, содержащую до миллиона его модификаций, что позволяет обнаружить практически все полиморфные вирусы. Типичный представитель – программа Nod32.

4**. Программы-мониторы**, или модули многофункциональных программ. Позволяют постоянно за счет размещения в оперативной памяти компьютера контролировать все процессы в реальном времени, в течение всего сеанса работы пользователя. Мониторы входят в состав практически всех современных антивирусных программ.

5. **Эвристические доктора**. Программы, способные находить группу вирусов по каким-либо общим признакам, даже если они (вирусы) имеют разное внутреннее строение (разные сигнатуры). Типичный общий признак для большинства вирусов – несанкционированное копирование, которое доктора и фиксируют. В сочетании с поиском и удалением известных сигнатур можно найти ранее выявленные вирусы либо заподозрить новый неизвестный вирус. Эвристические подходы используют большинство современных антивирусных программ, лучшими являются отечественные DrWeb, AVP Касперского.

6. На особо опасных участках заражения используются **карантинные доктора** ("виртуальные песочницы"). Они позволяют вновь прибывшим на компьютер программам работать, но только в отдельной изолированной области памяти. За ними в это время наблюдают программы-доктора. Если в течение определенного времени "гости" не заявят о себе плохо, то карантин заканчивается и они пускаются в "общую компанию". В противном случае при подозрении "гости" удаляются с компьютера. Типичные представители карантинных докторов – программы семейства eSafeProtect, AVZ.

7. **Проактивная защита.** Представляется программами, которые кроме эвристического анализа проводят мониторинг системного реестра, работы приложений с оперативной памятью, контроль целостности наиболее важных системных файлов. Пример – антивирусный пакет AVP Касперского.

**Антивирусный сканер –** антивирусная программа, осуществляющая поиск известных вирусов по маске вируса путем сканирования файлов, секторов и системной памяти. Такие программы иногда называют антивирусными детекторами.

**Сигнатурой вируса**называется уникальная последовательность кода, специфическая для данного конкретного вируса и однозначно его идентифицирующая. Сигнатура может быть сплошной или разреженной. В случае разреженной сигнатуры между уникальными постоянными для данного вируса байтами кода могут находиться другие байты, нехарактерные для этого вируса. Поиск по маске вируса и есть поиск по разреженной сигнатуре. Таким образом, ***маской вируса***называется специфическая для данного конкретного вируса разреженная сигнатура, по которой ведется выявление вируса.

Так как программы-детекторы выявляют вирусы путем поиска характерных для вирусов участков кода (сигнатур), которые записаны в антивирусной базе программы, то известные вирусы обнаруживаются надежно, хотя процесс сканирования может занимать значительное время.

**Полиморфные вирусы** могут не содержать ни одного постоянного участка кода и простым сигнатурным поиском не могут быть выявлены. Обнаружение полиморфик-вирусов требует использования специальных методик, наиболее известной из которых является эмуляция процессора, «заставляющая» вирус выполнить расшифровку его тела, после чего вирус может быть обнаружен с помощью сигнатурного поиска.

Для выявления новых, ранее не наблюдавшихся видов и разновидностей вредоносных программ, сигнатуры которых отсутствуют в антивирусной базе, сканеры могут использовать алгоритмы эвристического анализа.

**Эвристический анализ**в антивирусных программах − анализ объектов с целью выявления в них последовательностей команд, возможно присущих вредоносной программе. Решение эвристического анализатора носит вероятностный характер, возможен и пропуск вредоносного кода, и «ложная тревога», причем стремление повысить вероятность обнаружения вредоносных программ неизбежно приводит к увеличению ошибочного детектирования несуществующего в действительности вредоносного кода. Несмотря на возможные ошибочные решения, эвристический анализ позволяет существенно повысить эффективность работы антивирусного сканера как по обнаружению новых видов вирусов, так и полиморфик-вирусов и вирус генераторов. Полиморфик-вирусы, которые не имеют постоянных сигнатур, эвристический анализатор может выявить по присущим им характерным алгоритмам. Вирус-генераторы, представляющие собой специализированные библиотеки, позволяющие конструировать вирусы с изменяющейся сигнатурой, могут детектироваться по вызовам внешних процедур.

**CRC-сканер**− антивирусная программа-ревизор, осуществляющая выявление вирусов по изменению ранее подсчитанных и запомненных CRC- сумм (контрольных сумм) файлов и системных секторов, а также других параметров файлов, которыми могут являться размер файла, дата и время создания или модификации и т. п.). При обнаружении несоответствий программа-ревизор выдает сообщение пользователю, который анализируя это сообщение, должен принять решение, чем обусловлены выявленные изменения − наличием вируса или другими причинами.

Достоинством CRC-сканеров является способность выявлять даже трудно детектируемые стелс-вирусы. Недостатком CRC-сканеров является неспособность обнаруживать вирусы в новых или восстанавливаемых из резервных копий файлах, в сообщениях электронной почты, а также в момент внедрения вируса в компьютер. Также CRC-сканеры не могут выявлять вирусы, которые запрограммированы заражать только вновь создаваемые файлы.

**Антивирусный монитор**– резидентная антивирусная программа, выявляющая вредоносные программы по характерным для них действиям. К действиям, которые перехватывает антивирусный монитор (еще называемый антивирусом-фильтром), относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочные секторы дисков, попытки программ остаться в памяти резидентно и другие действия, специфичные для размножающихся и активирующихся вирусов. Достоинством антивирусных мониторов является способность выявлять вирусы, в том числе прежде неизвестные, на ранней стадии размножения, недостатком – множество возможностей нейтрализации монитора и большое число ложных срабатываний. Антивирусные мониторы используются крайне редко, причем обычно в составе аппаратных компонентов компьютеров, например, как антивирусная защита BIOS.

**Иммунизатор**− антивирусная программа, блокирующая заражение определенным типом вируса путем модификации файлов, придающей им признаки заражения. Это обеспечивает защиту, но только от определенного вируса, так как вирус сочтет, что эти файлы уже инфицированы им ранее.

Существует разновидность иммунизаторов, которые записываются в конец файла и при запуске файла проверяют его на изменение, что позволяет выявлять вирусное заражение файла. Антивирусы-иммунизаторы не способны выявлять стелс-вирусы, а защиту могут обеспечить лишь от немногих типов вирусов, что обусловливает их крайне низкую эффективность.

Приведем перечень наиболее известных антивирусных программ:

• Антивирус Касперского;

• ESETNOD32;

• Avast! Professional Edition;

• AVG Anti-Virus Free Edition;

• Avira AntiVir Personal Edition;

• DrWeb Антивирус;

• F-Secure Anti-Virus;

• Norton AntiVirus;

• Panda Antivirus;

• Sophos Norman Virus Control;

• McAffee VirusScan.

Указать лучшую из перечисленных антивирусных программ невозможно по двум причинам.

Во-первых, у каждой программы свой принцип работы и свои "любимые типы" вредоносных программ. Как и для всех болезней человека нет единого лекарства, так и нельзя назвать универсальную антивирусную программу.

Во-вторых, в отличие от вредоносных программ антивирусные программы, к сожалению, несовместимы для одновременной установки на один компьютер и не могут работать одновременно.

По данным тестирования, проведенного многими группами программистов, можно условно определить лучших в отдельных "антивирусных" группах:

• лучший (самый быстрый) сканер – ESET NOD32;

• лучший эвристик – Avira AntiVir Personal Edition или Dr Web;

• лучший проактив – Антивирус Касперского.