1. **ЗАЩИТА СУЩЕСТВУЮЩИХ ПРОГРАММ**

В настоящее время, большинство вредоносных программ, написано под операционную систему Windows. Частично, такая ситуация сложилась по причине её популярности, а так же из-за простоты работы с ней. Даже начинающие пользователи не испытывают сложностей с освоением основных функций данной системы, но совершенно не заботясь о защите. Этим и пользуется большинство вирусописателей, разрабатывая хитроумные алгоритмы заражения файлов. Единственный эффективный метод защиты существующих программ – это, по возможности, избегать заражения операционной системы. Но, к сожалению, это не всегда получается сделать. Поэтому приходится принимать дополнительные меры защиты информации.

И в первую очередь – это резервная архивация данных. Абсолютное большинство вредоносных программ не могут заразить исполняемые файлы, находящиеся в архивах. Поэтому рекомендуется все установочные файлы программ заархивировать, либо записать на компакт-диск. Так же, можно создать резервную копию операционной системы, так называемый *образ*. Он, по сути, ничем не отличается от архива, за исключением некоторых особенностей. И в случае, если операционная система повреждена и не загружается, не составит труда восстановить её из образа. Наиболее популярными утилитами, для создания образов системы, являются Acronis True Image, Norton Ghost, Nero BackItUp. Ещё, можно воспользоваться встроенной функцией *восстановления системы.* Правда, как показывает практика, в большинстве случаев, она неэффективна.

Далее, по степени эффективности защиты данных, следует визуальный контроль поведения системы в целом, контроль действий установленных программ и своевременная установка обновлений системы. Данные методы включают в себя периодическую проверку запущенных процессов. При обнаружении подозрительных процессов, работающих в фоновом режиме и никак себя не проявляющих, полезно поискать описание данных процессов в глобальной сети интернет, и проверить их антивирусным сканером. Также должна насторожить излишняя активность жесткого диска, при отсутствии каких либо причин. Затем, следует регулярно проверять области автозагрузки программ на наличие незнакомых. Будет полезным отключение такой службы, как Telnet и функций удалённого доступа и управления компьютером. С помощью уязвимостей в этих местах, возможен как и ручной взлом компьютера хакером, так и с проникновение сетевых червей. Также в Windows Vista появился весьма действенный механизм защиты от вредоносных программ - *Контроль учетных записей (UAC).* В состав UAC входят несколько технологий: учетная запись защищенного администратора (PA), запросы на повышение прав, виртуализация реестра, виртуализация файловой системы и уровни целостности Windows.

И, конечно, не обойтись без антивирусного программного обеспечения. В основном, большинство программ этого типа включает в себя следующие технологии:

* *Обнаружение, основанное на сигнатурах* — метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к базе данных с известными вирусами, составленной авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в базе, программа может заняться выполнением одного из нескольких действий, таких как удаление файла, отправка в карантин или удаления вредоносного кода из файла.
* *Проактивная защита* - метод работы программы, основанный на предотвращении заражения системы пользователя неизвестными вредоносными программами либо самомодифицирующимися вирусами. Метод включает в себя эвристический анализ, эмуляцию кода, анализ поведения, виртуализацию рабочего окружения.
* *Sandbox (песочница)* – сравнительно новая технология, направленная на безопасный запуск и анализ подозрительного исполняемого файла.
* *Сетевой экран (Фаервол, Брендмаузер)* — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Является наиболее эффективным средством борьбы с червями.

Также существует множество дополнительных технологий, присущих каждому отдельному антивирусу и каждая из них, является эффективной в своей области применения.

Большинство антивирусов, в настоящее время, являются платными, так как над разработкой базы данных вирусов, анализом вредоносных кодов и обработкой ошибок и улучшений программы трудится огромное количество людей. Но существуют и бесплатные продукты, такие как AVZ и Comodo Internet Security. Возможно, они и не столь совершенны, как их платные аналоги, но и они обеспечивают достаточный уровень защиты от большинства вредоносных программ.