

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/doklad/346675>

**Тип работы:** Доклад

**Предмет:** Информационные технологии

Содержание

Введение.....	3
1.Методы антивирусной защиты.....	4
2. Антивирусная профилактика.....	7
Заключение.....	10
Список литературы.....	11

Введение

Защита информации - мероприятия, направленные на предотвращение утечки защищенной информации, несанкционированного и непреднамеренного воздействия на защищенную информацию.

Актуальность темы исследования

Защита информации от несанкционированного доступа - деятельность, направленная на предотвращение доступа к защищенной информации в нарушение установленных прав и/или правил изменения информации, ведущая к искажению, уничтожению, копированию, блокированию доступа к информации, а также потеря, разрушение или выход из строя носителя информации.

1.Методы антивирусной защиты

Основным средством борьбы с вирусами были и остаются антивирусные программы. Вы можете использовать антивирусные( антивирусные) программы, не имея представления о том, как они организованы. Однако, не разобравшись в принципах работы антивирусного устройства, не зная типов вирусов, а также путей их распространения, невозможно организовать надежную защиту компьютера. В результате компьютер может быть заражен, даже если на нем установлен антивирус.

Сегодня используется несколько фундаментальных методов обнаружения и защиты от вирусов:

оцифровывание;

эвристический анализ;

использование антивирусных мониторов;

обнаружение изменений;

используйте антивирусы, встроенные в BIOS компьютера.

Кроме того, почти все антивирусные программы позволяют автоматически восстанавливать зараженные программы и загрузочные сектора. Конечно, если это возможно.

Сканирование

Самый простой метод проверки на вирусы заключается в том, что антивирусная программа систематически сканирует проверяемые файлы на наличие известных сигнатур вирусов. Под сигнатурой понимается уникальная последовательность байтов, принадлежащая вирусу и отсутствующая в других программах. Антивирусные сканеры могут обнаруживать только те вирусы, которые уже известны и изучены, для которых была установлена сигнатура. Использование простых программ сканирования не защищает ваш компьютер от проникновения новых вирусов.

Для зашифрованных и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить сигнатуру. Следовательно, простые антивирусные сканеры не могут обнаруживать полиморфные вирусы.

Эвристический анализ

Эвристический анализ позволяет обнаруживать неизвестные вирусы без предварительного сбора данных о файловой системе, как того требует, например, метод обнаружения изменений, описанный ниже.

2. Антивирусная профилактика

Давно известны следующие рекомендации, позволяющие снизить вероятность заражения компьютера: вам необходимо установить антивирусное программное обеспечение и регулярно обновлять его, устанавливая новую версию;

с помощью такого антивирусного программного обеспечения необходимо периодически проверять жесткие диски компьютера на наличие вирусов, запуская антивирусные программы для проверки файлов, памяти и системных областей;

использовать антивирусные программы для управления на входе всеми файлами, поступающими из компьютерных сетей и со съемных носителей (дискет, компакт-дисков);

после распаковки архивов, в том числе старых, немедленно проверьте их содержимое;

защита гибких дисков от записи при работе на других компьютерах, Если вы не планируете записывать на них;

включить антивирусную защиту системной области диска в конфигурационном BIOS.

Таким образом, основная часть профилактики заключается в правильном использовании антивирусных программ.

В настоящее время возросла доля сетевых вирусов-червей, использующих Интернет для своего размножения. Следовательно, помимо предыдущих рекомендаций, другие:

установите и настройте антивирусную программу для электронной почты (электронная почта) для автоматического сканирования, она может быть частью общего антивирусного пакета;

не открывайте файлы, прикрепленные к электронным письмам, средствами автозапуска программ операционной системы (например, для Windows - не применяйте к этим файлам двойной щелчок); вместо этого скопируйте файл, проверьте его с помощью антивируса, затем откройте-в из прикладной программы;

установите программу под названием брандмауэр (firewall), ее цель-предотвратить скрытый выход вирусов и других нежелательных программ в интернет;

не используйте интернет - инструменты, которые автоматически устанавливают программы, отклоняйте предложения по загрузке файлов в случае подозрительного происхождения;

регулярно устанавливайте и используйте программное обеспечение для обнаружения шпионских программ (которые не являются вирусами, но передают информацию через Интернет незаметно для пользователя).

Вышесказанное применимо к любому персональному компьютеру. В компаниях и организациях ИТ-специалисты обычно выполняют ограниченное количество задач.

## Заключение

Из истории компьютерной вирусологии ясно, что любая оригинальная компьютерная разработка требует от создателей антивирусов адаптации к новым технологиям, постоянного совершенствования антивирусных программ.

Основными способами проникновения вирусов являются съемные диски и компьютерные сети. Чтобы этого избежать, соблюдайте защитные меры. Кроме того, было разработано несколько типов специальных программ, называемых антивирусами, для обнаружения, удаления и защиты от компьютерных вирусов.

## Список литературы:

1. Жадаев, А.Г. Антивирусная защита ПК. От чайника к пользователю / А.Г. Жадаев. - М.: БХВ-Петербург, 2020. - 626 с.
2. Жадаев, Александр Антивирусная защита ПК. От "чайника" к пользователю / Александр Жадаев. - М.: БХВ-Петербург, 2020. - 224 с.
3. Козицкий, С. С. Англо-русский словарь по охране труда и средствам индивидуальной защиты / С.С. Козицкий. - М.: НЦ ЭНАС, 2021. - 336 с.

*Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:*

<https://stuservis.ru/doklad/346675>