**MINISTERU EDUCAȚIEI, CULTURII ȘI CERCETĂRII UNIVERSITATEA DE STAT „ALECU RUSSO” DIN BĂLŢI  
FACULTATEA DE ŞTIINŢE REALE, ECONOMICE ȘI ALE MEDIULUI CATEDRA DE MATEMATICĂ ȘI INFORMATICĂ**

**БЕЗОПАСНОСТЬ КОМПЬЮТЕРА. СИСТЕМНЫЙ АНТИВИРУС**

**РЕФЕРАТ ПО «INFORMATICA GENERALA»**

Autor:

Studentul grupei is11z

Davidov Ecaterina

Conducator stiintific:

Olesea Skutnitki

Magistru, asist. Univ.

**BALTI,2022**

ОГЛАВЛЕНИЕ

1. **Антивирусная программа**
2. **История создания антивируса**

**ПЕРВЫЕ САМОВОСПРОИЗВОДЯЩИЕСЯ ПРОГРАММЫ**

### ДЖО ДЕЛЛИНДЖЕР

### ГРЯЗНАЯ ДЮЖИНА

### ПЕРВЫЕ АНТИВИРУСЫ

1. **Основные меры защиты от вирусов**
2. **История создания вируса**

**Первые вирусные эпидемии**

### Brain и Jerusalem

1. **Антивирусные программы**

**Разновидности антивирусных программ**

1. **Популярные антивирусные программы**
2. **Библиография**

1. АНТИВИРУСНАЯ ПРОГРАММА

Антивирусная программа (антивирус) -- это специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики -- предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Компьютерные вирусы - это небольшие программы, которые предназначены для вмешательства в работу компьютера; для записи, повреждения или удаления данных; или для распространения на другие компьютеры и через Интернет.

Чтобы защититься от новых вирусов, необходимо регулярно обновлять антивирусное ПО. Для большинства типов антивирусных программ можно настроить автоматическое обновление.

В то время как антивирусное программное обеспечение, предназначенное в первую очередь, для защиты компьютеров от вирусов, многие антивирусные программы, теперь призваны защищать нашу систему, от других видов вредоносных, шпионских программ, рекламных баннеров и т.д.

Некоторые антивирусные утилиты могут поставляться совместно с брандмауэром, что позволяет предотвратить несанкционированный доступ к вашему компьютеру.

2. ИСТОРИЯ СОЗДАНИЯ ПЕРВЫХ АНТИВИРУСОВ

ПЕРВЫЕ САМОВОСПРОИЗВОДЯЩИЕСЯ ПРОГРАММЫ

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения [Джон фон Нейман](https://ru.wikipedia.org/wiki/%D0%94%D0%B6%D0%BE%D0%BD_%D1%84%D0%BE%D0%BD_%D0%9D%D0%B5%D0%B9%D0%BC%D0%B0%D0%BD), который в [1951 году](https://ru.wikipedia.org/wiki/1951_%D0%B3%D0%BE%D0%B4) предложил метод создания таких механизмов. Первой публикацией, посвящённой созданию самовоспроизводящихся систем, является статья Л. С. Пенроуз в соавторстве со своим отцом, нобелевским лауреатом по физике Р. Пенроузом, о самовоспроизводящихся механических структурах, опубликованная в [1957 году](https://ru.wikipedia.org/wiki/1957_%D0%B3%D0%BE%D0%B4) американским журналом [Nature](https://ru.wikipedia.org/wiki/Nature). В этой статье, наряду с примерами чисто механических конструкций, была приведена некая двумерная модель подобных структур, способных к активации, захвату и освобождению. По материалам этой статьи Ф. Ж. Шталь (F. G. Stahl) запрограммировал на машинном языке ЭВМ [IBM 650](https://ru.wikipedia.org/wiki/IBM_650) биокибернетическую модель, в которой существа двигались, питаясь ненулевыми словами. При поедании некоторого числа символов существо размножалось, причём дочерние механизмы могли мутировать. Если кибернетическое существо двигалось определённое время без питания, оно погибало.

В [1961 году](https://ru.wikipedia.org/wiki/1961_%D0%B3%D0%BE%D0%B4) [В. А. Высотский](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%81%D0%BE%D1%82%D1%81%D0%BA%D0%B8%D0%B9,_%D0%92%D0%B8%D0%BA%D1%82%D0%BE%D1%80_%D0%90%D0%BB%D0%B5%D0%BA%D1%81%D0%B0%D0%BD%D0%B4%D1%80%D0%BE%D0%B2%D0%B8%D1%87), [Дуглас Макилрой](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BA%D0%B8%D0%BB%D1%80%D0%BE%D0%B9,_%D0%94%D1%83%D0%B3%D0%BB%D0%B0%D1%81) и [Роберт Моррис](https://ru.wikipedia.org/w/index.php?title=%D0%9C%D0%BE%D1%80%D1%80%D0%B8%D1%81,_%D0%A0%D0%BE%D0%B1%D0%B5%D1%80%D1%82_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84)&action=edit&redlink=1)из фирмы [Bell Labs](https://ru.wikipedia.org/wiki/Bell_Labs) (США) изобрели необычную игру «[Дарвин](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%80%D0%B2%D0%B8%D0%BD_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B8%D0%B3%D1%80%D0%B0))», в которой несколько [ассемблерных](https://ru.wikipedia.org/wiki/%D0%AF%D0%B7%D1%8B%D0%BA_%D0%B0%D1%81%D1%81%D0%B5%D0%BC%D0%B1%D0%BB%D0%B5%D1%80%D0%B0) программ, названных «организмами», загружались в память компьютера. Организмы, созданные одним игроком (то есть принадлежащие к одному виду), должны были уничтожать представителей другого вида и захватывать жизненное пространство. Победителем считался тот игрок, чьи организмы захватывали всю память или набирали наибольшее количество очков.

В феврале [1980 года](https://ru.wikipedia.org/wiki/1980_%D0%B3%D0%BE%D0%B4) студент Дортмундского университета Юрген Краус подготовил дипломную работу по теме «Самовоспроизводящиеся программы», в которой помимо теории приводились так же и листинги строго самовоспроизводящихся программ (которые вирусами на самом деле не являются) для компьютера [Siemens](https://ru.wikipedia.org/wiki/Siemens).

Появление первых компьютерных вирусов зачастую ошибочно относят к [1970-м](https://ru.wikipedia.org/wiki/1970-%D0%B5) и даже [1960-м годам](https://ru.wikipedia.org/wiki/1960-%D0%B5). Обычно упоминаются как «вирусы» такие программы, как [ANIMAL](https://ru.wikipedia.org/wiki/ANIMAL), [Creeper](https://ru.wikipedia.org/wiki/Creeper), [Cookie Monster](https://ru.wikipedia.org/wiki/Cookie_Monster) и [Xerox worm](https://ru.wikipedia.org/w/index.php?title=Xerox_worm&action=edit&redlink=1).

ELK CLONER

В [1981 году](https://ru.wikipedia.org/wiki/1981_%D0%B3%D0%BE%D0%B4) [Ричард Скрента](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B5%D0%BD%D1%82%D0%B0,_%D0%A0%D0%B8%D1%87%D0%B0%D1%80%D0%B4) написал один из первых [загрузочных вирусов](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BE%D1%87%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81) для ПЭВМ [Apple II](https://ru.wikipedia.org/wiki/Apple_II) — ELK CLONER. Он обнаруживал своё присутствие сообщением, содержащим небольшое стихотворение:

ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS

IT WILL INFILTRATE YOUR CHIPS

YES, IT'S CLONER

IT WILL STICK TO YOU LIKE GLUE

IT WILL MODIFY RAM, TOO

SEND IN THE CLONER!

ДЖО ДЕЛЛИНДЖЕР

Другие вирусы для Apple II были созданы студентом Техасского университета [A&M](https://ru.wikipedia.org/wiki/A%26M) [Джо Деллинджером](https://ru.wikipedia.org/w/index.php?title=%D0%94%D0%B6%D0%BE_%D0%94%D0%B5%D0%BB%D0%BB%D0%B8%D0%BD%D0%B4%D0%B6%D0%B5%D1%80&action=edit&redlink=1) в [1981 году](https://ru.wikipedia.org/wiki/1981_%D0%B3%D0%BE%D0%B4). Они были рассчитаны на операционную систему [Apple DOS](https://ru.wikipedia.org/wiki/Apple_DOS) 3.3 для этой ПЭВМ. Вторая версия этого вируса «ускользнула» от автора и начала распространяться по университету. Ошибка в вирусе вызывала подавление графики популярной игры под названием CONGO, и в течение нескольких недель все («пиратские») копии этой игры перестали работать. Для исправления ситуации автор запустил новый, исправленный вирус, предназначенный для «замещения» предыдущей версии. Обнаружить вирус можно было по наличию в памяти счётчика заражений: «(GEN 0000000 TAMU)», по смещению $B6E8, или в конце нулевого сектора заражённого диска.

ГРЯЗНАЯ ДЮЖИНА

В [1985 году](https://ru.wikipedia.org/wiki/1985_%D0%B3%D0%BE%D0%B4) Том Нефф ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Tom Neff) начал распространять по различным [BBS](https://ru.wikipedia.org/wiki/BBS) список «Грязная дюжина — список опасных загружаемых программ» ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) The Dirty Dozen — An Unloaded Program Alert List), в котором были перечислены известные на тот момент программы-вандалы. В дальнейшем этот список, включающий большинство выявленных троянских программ и «взломанные» или переименованные копии коммерческого программного обеспечения для [MS-DOS](https://ru.wikipedia.org/wiki/MS-DOS), стал широко известен под кратким названием «грязная дюжина» ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) dirty dozen).

ПЕРВЫЕ АНТИВИРУСЫ

Первые [антивирусные утилиты](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D1%8B%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B) появились зимой [1984 года](https://ru.wikipedia.org/wiki/1984_%D0%B3%D0%BE%D0%B4). [Энди Хопкинс](https://ru.wikipedia.org/w/index.php?title=%D0%AD%D0%BD%D0%B4%D0%B8_%D0%A5%D0%BE%D0%BF%D0%BA%D0%B8%D0%BD%D1%81&action=edit&redlink=1) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Andy Hopkins) написал программы [CHK4BOMB](https://ru.wikipedia.org/w/index.php?title=CHK4BOMB&action=edit&redlink=1) и [BOMBSQAD](https://ru.wikipedia.org/w/index.php?title=BOMBSQAD&action=edit&redlink=1). CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявляла все текстовые сообщения и «подозрительные» участки кода (команды прямой записи на диск и др.). Благодаря своей простоте (фактически использовался только контекстный поиск) и эффективности CHK4BOMB получила значительную популярность.

Программа BOMBSQAD.COM перехватывает операции записи и форматирования, выполняемые через [BIOS](https://ru.wikipedia.org/wiki/BIOS). При выявлении запрещённой операции можно разрешить её выполнение. Спрос, как известно, рождает предложение, и первая резидентная антивирусная программа под названием DPROTECT, разработанная программистом и основателем американской софтверной компании GEE WIZ Sofware Company Ги Вонгом, появилась в начале 1985 года. Программа DPROTECT распространялась бесплатно, однако желающие могли сделать добровольное пожертвование в размере пяти долларов. Приложение не использовало в своей работе вирусные базы, содержащие сигнатуры вредоносных программ, а отслеживало активность запущенных программ, перехватывая обращения к файловой системе. Таким образом резидентный монитор DPROTECT позволял обезопасить защищаемый компьютер от деструктивных действий программ, которые могли, например, отформатировать диск или испортить загрузочную запись.

Вторая половина 80-х годов ознаменовалась широкой экспансией на международном рынке персональных компьютеров семейства IBM PC и ростом популярности операционной системы MS-DOS. К этому же периоду относятся и первые масштабные вирусные эпидемии: летом 1987 года 18 тысяч компьютеров оказались заражены стелс-вирусом Pakistani Brain, разработанным братьями Амджатом и Базитом Алви — с помощью этой вредоносной программы они пытались отомстить пиратам, воровавшим программное обеспечение у их фирмы. Написанный студентом из Новой Зеландии вирус Stoned, получивший распространение в том же 1987 году, заражал загрузочную запись ПК и блокируя запуск ОС. От этой напасти пострадало несколько тысяч компьютеров по всему миру. А в пятницу, 13 мая 1988 года пользователи познакомились с вирусом Jerusalem, уничтожавшим приложения при попытке их запуска. Эта вредоносная программа вызвала настоящую пандемию, распространившись на территории не только США, но также Европы и Азии. Разумеется, отыскались толковые парни, очень быстро осознавшие, что на компьютерной безопасности можно неплохо заработать — одним из них оказался простой программист из Lockheed Corporation по имени Джон Макафи, выпустивший в 1988 году коммерческий продукт под названием McAfee Virus Scan, а в 1989 году основавший компанию имени себя. Вскоре, почувствовав запах прибыли, подтянулись и другие игроки: в 1991 году состоялся релиз первой версии приложения под названием Norton AntiVirus/

На отечественном рынке истинным первопроходцем стал Дмитрий Николаевич Лозинский, разработавший в 1988 году, практически одновременно с Макафи, антивирусную программу-сканер Aidstest, использовавшую технологию сигнатурного поиска угроз. Приложение, дистрибуцией которого занималась компания «Диалог Наука», быстро завоевало заслуженную популярность у пользователей, на долгие годы став своего рода стандартом антивирусного ПО. Дмитрий Николаевич и по сей день вносит ощутимый вклад в борьбу с вирусными угрозами — в качестве одного из ведущих сотрудников компании «Доктор Веб».

3. ИСТОРИЯ СОЗДАНИЯ ВИРУСА

Очередным этапом развития вирусов считается [1987 год](https://ru.wikipedia.org/wiki/1987_%D0%B3%D0%BE%D0%B4). К этому моменту получили широкое распространение сравнительно дешёвые компьютеры IBM PC, что привело к резкому увеличению масштаба заражения компьютерными вирусами. Именно в 1987 вспыхнули сразу три крупные эпидемии компьютерных вирусов.

На протяжении уже более 60 лет компьютерные вирусы находятся в сфере коллективного  
человеческого сознания. То, что однажды было лишь кибер-вандализмом, быстро превратилось в киберпреступление. Быстро развиваются черви, троянцы и вирусы. Хакеры мотивированы и умны, они всегда стремятся тестировать на прочность системы и код, расширять границы доступных им методов и изобретать новые способы заражения. В будущем киберпреступники, вероятно, будут чаще взламывать PoS-терминалы – в качестве хорошего примера можно привести недавний троянец удаленного доступа [Moker](https://threatpost.com/new-moker-rat-bypasses-detection/114948/). Этот новый троянец сложно обнаружить, тяжело удалить – он обходит все известные механизмы защиты. Ничего не известно наверняка; постоянные перемены – в самой природе постоянной борьбы между киберпреступниками и системами защиты.

4. ОСНОВНЫЕ МЕРЫ ЗАЩИТЫ ОТ ВИРУСОВ

Меры по защите от вирусов

Для защиты следует:

• использовать датчик поиска вирусов для автоматической проверки компьютера на вирусы во время работы;

• использовать датчик описаний вирусов для автоматического обновления описаний вирусов. Это даст уверенность в том, что компьютер будет защищен от самых новейших вирусов;

• приобрести и использовать хорошую программу по обнаружению и удалению вирусов;

• периодически создавать резервные копии жестких дисков.

Антивирусные программы

Программы, позволяющие обнаружить и уничтожить вирусы, называют *антивирусными программами.* Рассмотрим основные виды антивирусных программ.

Программы-детекторы

К ним относятся такие программы, которые осуществляют *поиск характерной* (для конкретного типа вирусов) *последовательности байтов в оперативной памяти* и при их обнаружении выдают соответствующее сообщение. Однако такие последовательности могут быть известны только разработчикам вирусных программ.

Программы доктора (фаги, или программы-вакцины)

Фаги находят не только зараженные вирусами файлы, но и удаляют из них тело программы вируса, возвращая файл в исходное, рабочее состояние. Среди фагов выделяют *полифаги*, предназначенные для поиска и уничтожения большого количества вирусов. К полифагам относятся следующие известные программы: Aidstest, Scan, Norton Antivirus, Doctor Web и др.

Программы-ревизоры

Эти программы относятся к наиболее надежным средствам защиты от вирусов. В их памяти хранятся незаряженные вирусом программы, каталоги, системные области дисков. В процессе работы компьютера (как правило, после загрузки операционной системы) текущее состояние сравнивается с исходным по таким параметрам, как длина файла, контрольная сумма файла, дата и время модификации. Примером такой программы является программа *Adinf* фирмы "Диалог-Наука".

Программы-фильтры, или "сторожа"

К этому виду программ относятся небольшие резидентные (постоянно находящиеся в памяти) программы, предназначенные для обнаружения таких характерных для вирусов действий компьютера, как изменение атрибутов файлов, попытки коррекции файлов с расширение СОМ и EXE; запись в загрузочные сектора диска, прямая запись на диск по абсолютному адресу; загрузка резидентной программы.

"Сторож" оповещает пользователя сообщением о попытке какой-либо программы произвести указанные действия с предложением их запрета или разрешения. Программы-фильтры способны только обнаружить, но не уничтожают вирусы.

Вакцины, или иммунизаторы

Эти резидентные программы предотвращают заражение файлов. Вакцина модифицирует программу или диск таким образом, чтобы они были работоспособны, по выглядели как зараженные. Вакцинация возможна только от известных вирусов. В настоящее время их применение ограничено.

Для защиты от вирусов используют три группы методов:

Методы, основанные на *анализе содержимого файлов* (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.

Методы, основанные на *отслеживании поведения программ* при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, ибо при его программной эмуляции.

Методы *регламентации порядка работы* с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности.

**Метод сканирования сигнатур** ([сигнатурный анализ](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%B3%D0%BD%D0%B0%D1%82%D1%83%D1%80%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7), сигнатурный метод) основан на поиске в файлах уникальной последовательности байтов — **сигнатуры**, характерной для определенного вируса. Для каждого вновь обнаруженного вируса специалистами антивирусной лаборатории выполняется анализ кода, на основании которого определяется его сигнатура. Полученный кодовый фрагмент помещают в специальную базу данных вирусных сигнатур, с которой работает антивирусная программа. Достоинством данного метода является относительно низкая доля ложных срабатываний, а главным недостатком — принципиальная невозможность обнаружения в системе нового вируса, для которого отсутствует сигнатура в базе данных антивирусной программы, поэтому требуется своевременная актуализация базы данных сигнатур.

**Метод контроля целостности** основывается на том, что любое неожиданное и беспричинное изменение данных на диске является подозрительным событием, требующим особого внимания антивирусной системы. Вирус обязательно оставляет свидетельства своего пребывания (изменение данных существующих (особенно системных или исполняемых) файлов, появление новых исполняемых файлов и т. д.). Факт изменения данных — *нарушение целостности* — легко устанавливается путем сравнения [контрольной суммы](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D1%83%D0%BC%D0%BC%D0%B0) (дайджеста), заранее подсчитанной для исходного состояния тестируемого кода, и контрольной суммы (дайджеста) текущего состояния тестируемого кода. Если они не совпадают, значит, целостность нарушена и имеются все основания провести для этого кода дополнительную проверку, например, путем сканирования вирусных сигнатур. Указанный метод работает быстрее метода сканирования сигнатур, поскольку подсчет контрольных сумм требует меньше вычислений, чем операции побайтового сравнения кодовых фрагментов, кроме того он позволяет обнаруживать следы деятельности любых, в том числе неизвестных, вирусов, для которых в базе данных еще нет сигнатур.

**Метод сканирования подозрительных команд** ([эвристическое сканирование](https://ru.wikipedia.org/wiki/%D0%AD%D0%B2%D1%80%D0%B8%D1%81%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D1%81%D0%BA%D0%B0%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), эвристический метод) основан на выявлении в сканируемом файле некоторого числа подозрительных команд и(или) признаков подозрительных кодовых последовательностей (например, команда форматирования жесткого диска или функция внедрения в выполняющийся процесс или исполняемый код). После этого делается предположение о вредоносной сущности файла и предпринимаются дополнительные действия по его проверке. Этот метод обладает хорошим быстродействием, но довольно часто он не способен выявлять новые вирус.

**Метод отслеживания поведения программ** принципиально отличается от методов сканирования содержимого файлов, упомянутых ранее. Этот метод основан на анализе поведения запущенных программ, сравнимый с поимкой преступника «за руку» на месте преступления. Антивирусные средства данного типа часто требуют активного участия пользователя, призванного принимать решения в ответ на многочисленные предупреждения системы, значительная часть которых может оказаться впоследствии ложными тревогами. Частота ложных срабатываний (подозрение на вирус для безвредного файла или пропуск вредоносного файла) при превышении определенного порога делает этот метод неэффективным, а пользователь может перестать реагировать на предупреждения или выбрать оптимистическую стратегию (разрешать все действия всем запускаемым программам или отключить данную функцию антивирусного средства). При использовании антивирусных систем, анализирующих поведение программ, всегда существует риск выполнения команд вирусного кода, способных нанести ущерб защищаемому компьютеру или сети. Для устранения подобного недостатка позднее был разработан [метод эмуляции](https://ru.wikipedia.org/wiki/%D0%AD%D0%BC%D1%83%D0%BB%D1%8F%D1%86%D0%B8%D1%8F) (имитации), позволяющий запускать тестируемую программу в искусственно созданной (виртуальной) среде, которую часто называют [песочницей](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%81%D0%BE%D1%87%D0%BD%D0%B8%D1%86%D0%B0_(%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) ([sandbox](https://ru.wikipedia.org/wiki/Sandbox)), без опасности повреждения информационного окружения. Использование методов анализа поведения программ показало их высокую эффективность при обнаружении как известных, так и неизвестных вредоносных программ[]](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0#cite_note-:1-2).

5. ВЫБОР АНТИВИРУСА

1. Антивирусное ПО является основным элементом защиты системы, файлов, личной информации. Такие решения призваны защищать ПК по всем позициям – начиная от несанкционированного вмешательства в системные файлы до ознакомления с содержимым веб-страниц. Если такая защита не будет работать, компьютер станет уязвимым, а это очень опасно. Разработчики атак постоянно совершенствуются, пытаясь обойти даже лучшую защиту, а потому крайне важно, чтобы обновления совершались своевременно. Ведущие разработчики предлагают исправления уже через час после выявления уязвимости и даже быстрее. Сегодня особую важность могут играть облачные решения – постоянная работа с сервером ускоряет процесс запуска новых механизмов защиты и дает возможность оперативнее реагировать на угрозы.

2. Не менее важен и поведенческий анализ – благодаря ему антивирусы распознают различные угрозы, обнаруживаемые в ПО. Опасность может оказаться различного уровня – от попыток замены ключей до применения настроек в браузерах и он обязательно должен присутствовать в вашем кандидате

3. Ну и самое важное ключ антивируса нужно покупать, а не скачивать с каких-то обменников, так как в этом случае вы автоматом подвергаетесь на опасность заражения вирусами своих девайсов, а если вы еще и работаете с домашнего устройства, то и безопасность копании на которую вы работаете!

Классификация антивирусных программ

Антивирусные программы подразделяются по исполнению (средствам блокирования) на:

* программные;
* программно-аппаратные.

По признаку размещения в оперативной памяти выделяют:

* резидентные (начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов);
* нерезидентные (запускаются по требованию пользователя или в соответствии с заданным для них расписанием).

6. Виды антивирусных программ

1. [**Norton Security**](https://softlist.com.ua/catalog/product-norton-security/)

Недавно представленный на рынке антивирус в состоянии обнаружить все варианты атак, среди которых и старые, и сверхновые. При этом запуск различного рода приложений замедляется всего на 8%, тогда как показатель, демонстрируемый другими вариантами, находится на уровне около 18%. Помимо этого производится незаметный пользователю анализ установленного ПО, загрузки и копирования файлов. Ложных тревог не наблюдается. Security 22, безусловно, является лучшим антивирусом 2020 года из предлагаемых для Windows. Нужно отметить, что у решения присутствуют встроенные функции, среди которых менеджер паролей, сообщение о попытках доступа к камере. Предлагается 10 ГБ облачного копирования для компьютера, в также возможность безопасного просмотра в анонимном режиме с использованием VPN.

2. [**BullGuard Internet Security**](https://softlist.com.ua/catalog/product-bullguard-internet-security/)

Вирусом обнаружено все вредоносное ПО, появившейся в сети за месяц до атаки, набрано 99,4% при выявлении уязвимости «нулевого дня», а также фишинга (показатель других антивирусов «дотягивает» лишь до 99,1%). Запуск приложений не замедляется, но установка слегка притормаживает (на 20% при 30% усредненного показателя).Из более чем миллиона тестов ложное срабатывание имело место всего дважды. Пользователь может применять встроенный веб-браузер, сканер, призванный обнаруживать уязвимости. В наличии механизмы родительского контроля и режим плеера – благодаря этому программа не мешает основной работе.

3. [**Avast Premium Security**](https://softlist.com.ua/catalog/product-avast-premium-security/)

Решение демонстрирует абсолютную эффективность при обнаружении онлайн-атак и борьбе с ними. Но при этом антивирус замедлил открытие сайтов практически на четверть при среднем показателе 18%. Приложения работают медленнее на 14% при среднем значении 10%, а скорость копирования снижается на 4% при среднем уровне в 2%.

В общем антивирус хорош. Он в состоянии защитить жесткий диск, носители DVD, портативные устройства. Среди возможностей – утилита File Shredder, позволяющая безопасно удалять файлы, Data Safe (шифрование личных данных и защита их паролем), защита веб-камеры и модуль, избавляющий от спама.

4. [**Avira Antivirus Pro**](https://softlist.com.ua/catalog/product-avira-antivirus-pro/)

Avira Antivirus Pro – мощное решение, и это не раз подтверждено проводившимися тестами. Антивирус в состоянии обезопасить систему от старых и сверхсовременных угроз вне зависимости от того, откуда они исходят. На открытие приложений и веб-сайтов он оказывает незначительное влияние (около 17%). Решением предлагается VPN, варианты оптимизации, менеджер паролей, возможность восстановить поврежденные файлы. Предлагается бесплатная и продвинутая оплачиваемая версия Avira Antivirus Pro 15.0.

5. Microsoft Windows Defender

Интересный факт: ряд проведенных тестов доказывает, что Microsoft [Windows](https://softlist.com.ua/catalog/product-windows-10/) Defender является антивирусной защитой, которая не хуже, чем платные версии программ. Защита от вредителей является 100%, при этом она практически не влияет на скорость копирования, использование приложений.

Минусом остается только установка, которая замедляется на 44%, в то время как другие решения демонстрируют более интересные показатели – около 33%. За время тестирования были созданы два ложных срабатывания. Благодаря функции SmartScreen обеспечивается защита от открытия фальшивых и зараженных сайтов. Сервис Find My Device дает возможность подключения к потерянному устройству, его блокировке и удалению данных.

6. [**Bitdefender Internet Security**](https://softlist.com.ua/catalog/product-bitdefender-internet-security-2019/)

Это отличный вариант защиты, известный еще по более ранним версиям. Минусы, конечно, есть: антивирус значительно замедляет открытие веб-сайтов. В ходе тестов он показал три ложных срабатывания: при установке ПО и при использовании приложений. Решение является надежным, его функционал дополнен рядом опций, среди которых родительский контроль, предоставление безопасного браузера, VPN. Предлагается и новый инструмент – Ransomware Repair, обеспечивая защиты личной информации, фото, документов и пр.

7. [**McAfee LiveSafe**](https://softlist.com.ua/catalog/product-mcafee-livesafe/)

Предлагаемый борец с вирусами является кросс-платформенным вариантом для обеспечения защиты различного типа устройств. Решение включает фаервол, возможность родительского контроля, наличие "облака". McAfee LiveSafe становится оптимальной защитой ПК, веб-серфинга, другой информации.

Один из лидеров продаж 2020, по причине того, что одним недорогим ключем вы можете закрыть вопрос безопасности всех девайсов у вас в доме и при этом по всем тестам он ничем не уступает своим конкурентам. Так же решения от McAfee сегодня лидируют на рынке по защите для бизнеса. Они имеют достаточно гибкие цены и огромный функционал, который сможет закрыть подробности любой компании. Подробнее о решениях [McAfee](https://softlist.com.ua/vendors/mcafee/) вы сможете узнать у наших сертифицированных специалистов.

8. [**ESET Internet Security**](https://softlist.com.ua/catalog/product-eset-internet-security/)

Интересное решение, предоставляющее возможность защиты с применением облачных и проактивных технологий. Присутствует фаервол, обеспечение безопасности платежей онлайн, защита домашней сети, предлагается осуществление родительского контроля. Это обновленный подход к безопасности ПК.

Благодаря наличию интеллектуальной системы пользователь постоянно информируется об атаках и вредоносных программах, которые в состоянии причинить вред компьютеру.

Антивирусное решение позволяет совместить минимальное влияние на систему с надежным уровнем защиты. Используются интеллектуальные варианты предотвращения атак рекламного ПО, «червей», «троянов» - системная производительность не снижается и работу прерывать не нужно. Антивирус набрал максиальное количество баллов у AV-TEST и не очень требователен к системным требованиям.

9. [**360 Total Security**](https://softlist.com.ua/catalog/product-360-total-security-premium/)

360 Total Security в версии Премиум – это надежный современный антивирус, обеспечивающий достойную защиту устройства от шифраторов, троянов, сетевых червей и пр. Используя его, не следует беспокоиться, приобретая товары в интернете, общаясь в социальных сетях, загружая файлы.

Гарантируется беспрецедентный уровень безопасности ПК. Антивирус позволяет настроить оптимальную производительность, очистив устройство от «мусора» и совершенно забыв о навязчивой рекламе.

10. [**Malwarebytes for Windows**](https://softlist.com.ua/catalog/product-malwarebytes-for-windows/)

Антивирус помогает обнаружить различные угрозы и избавить от них компьютер. Нужно отметить, что решение выделяется среди других вариантов широтой базу – в нее входят рекламные, шпионские программы, уязвимости любого уровня.

Программа предлагает несколько степеней защиты от вредоносного ПО, инструменты для очистки компьютера, оптимальные варианты обнаружения зловредов, систему защиты от рукитов. Это дает возможность эффективно применять единственное решение для защиты ПК, не прибегая ко многим. В течение двух недель Malwarebytes for Windows можно использовать совершенно бесплатно, но после возможности антивируса будут существенно ограничены.