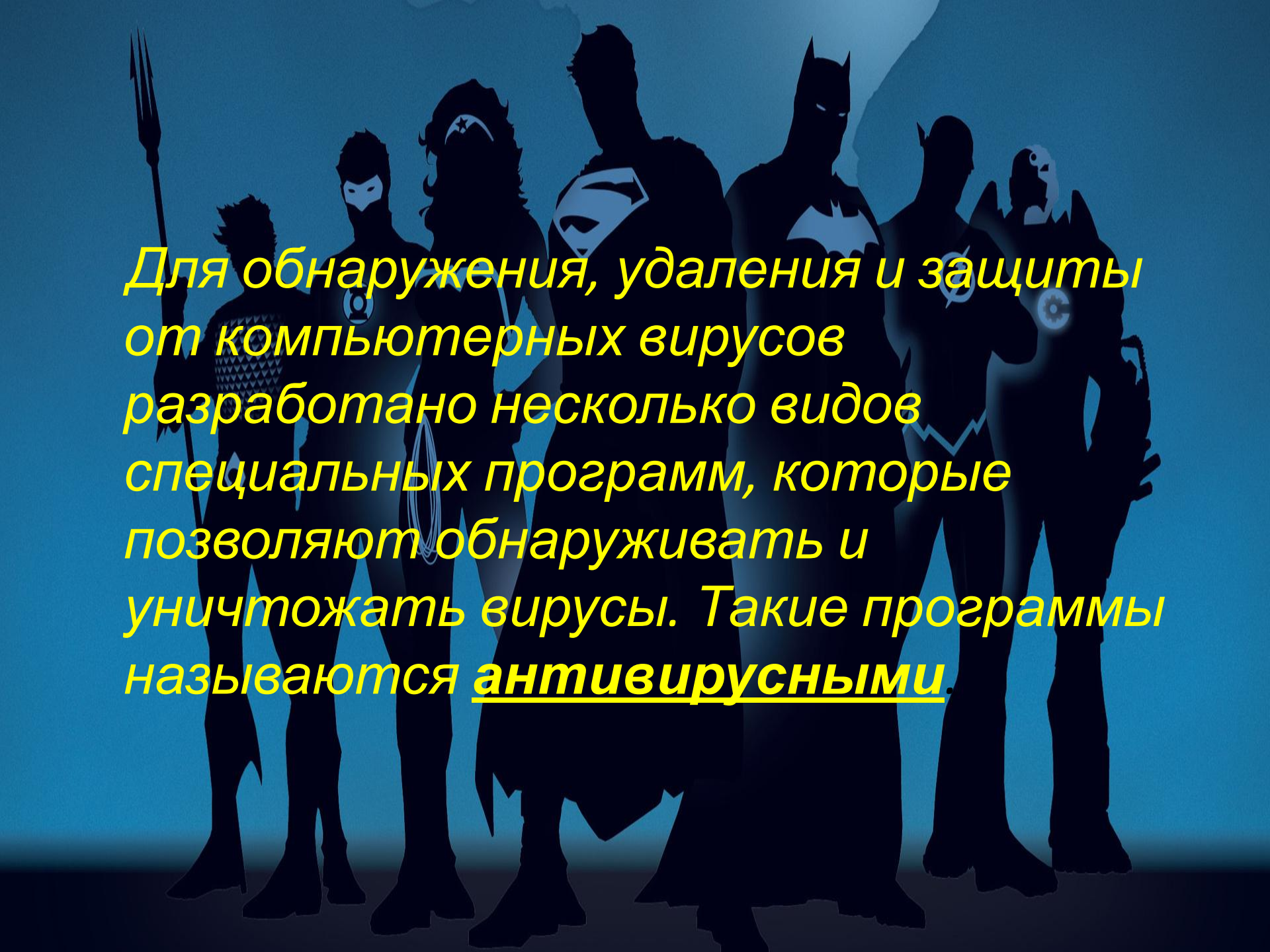
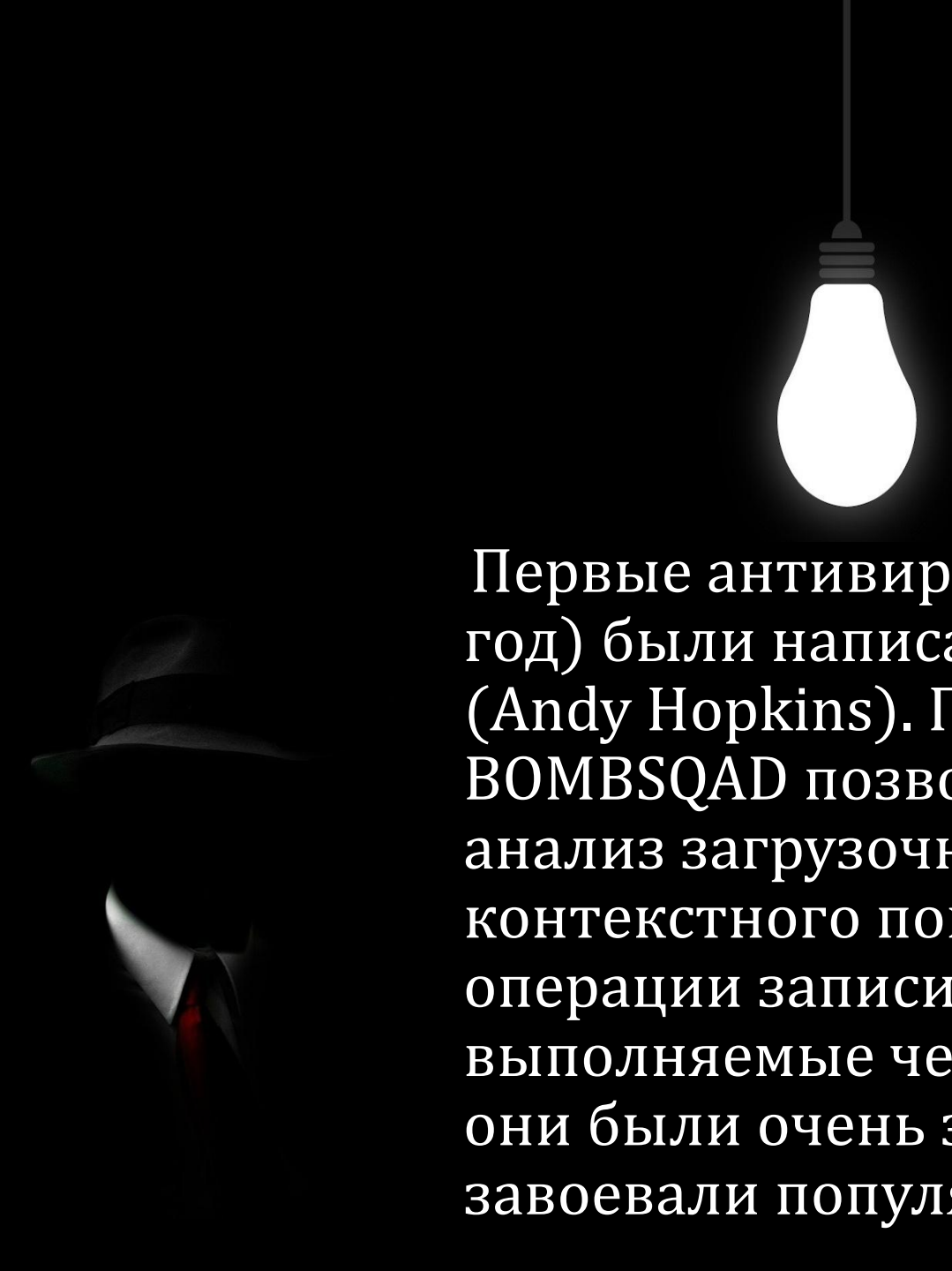
Виды антивирусных программ

Компьютерным вирусом *называется специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.*



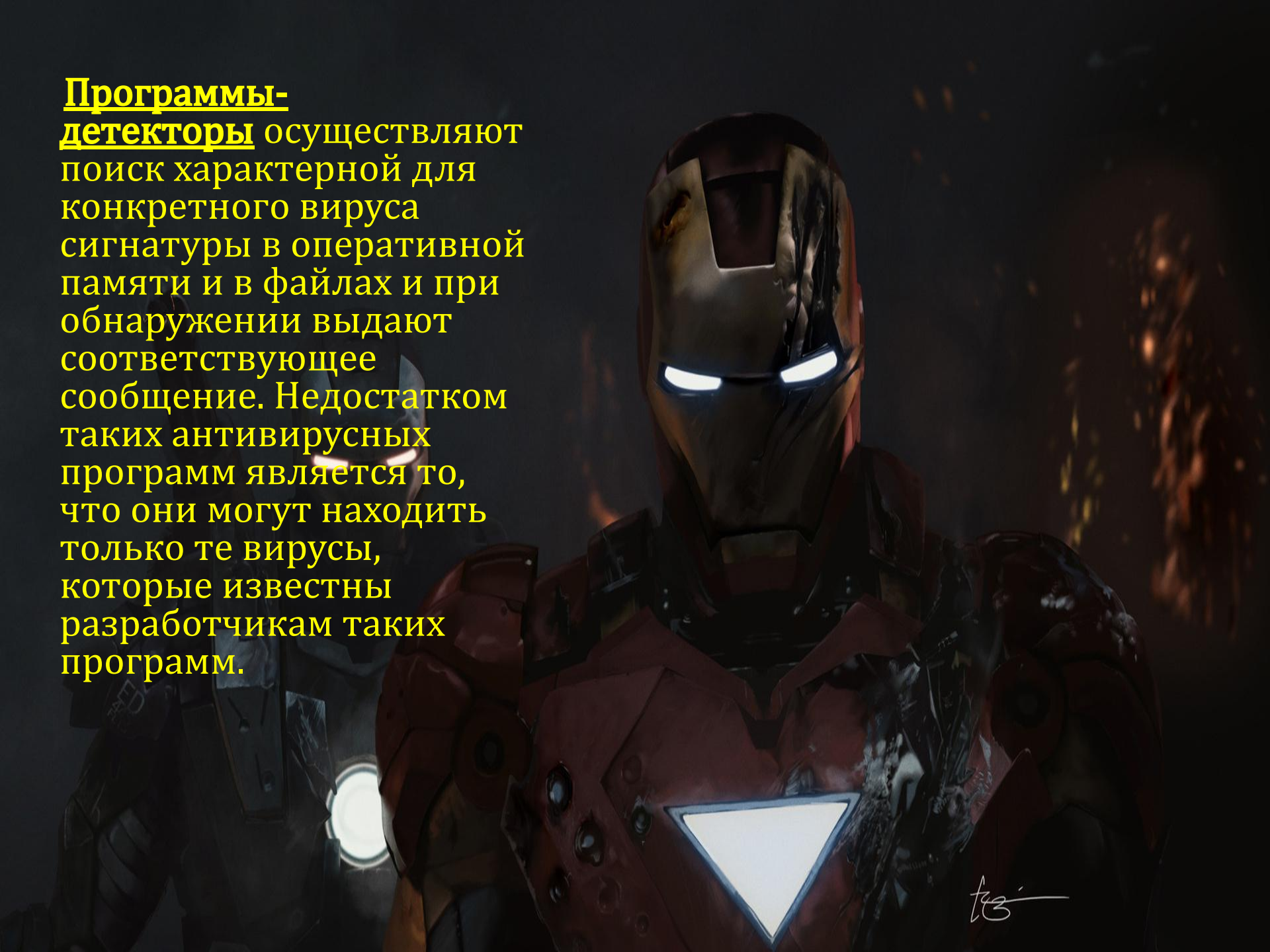
Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются ***антивирусными***.



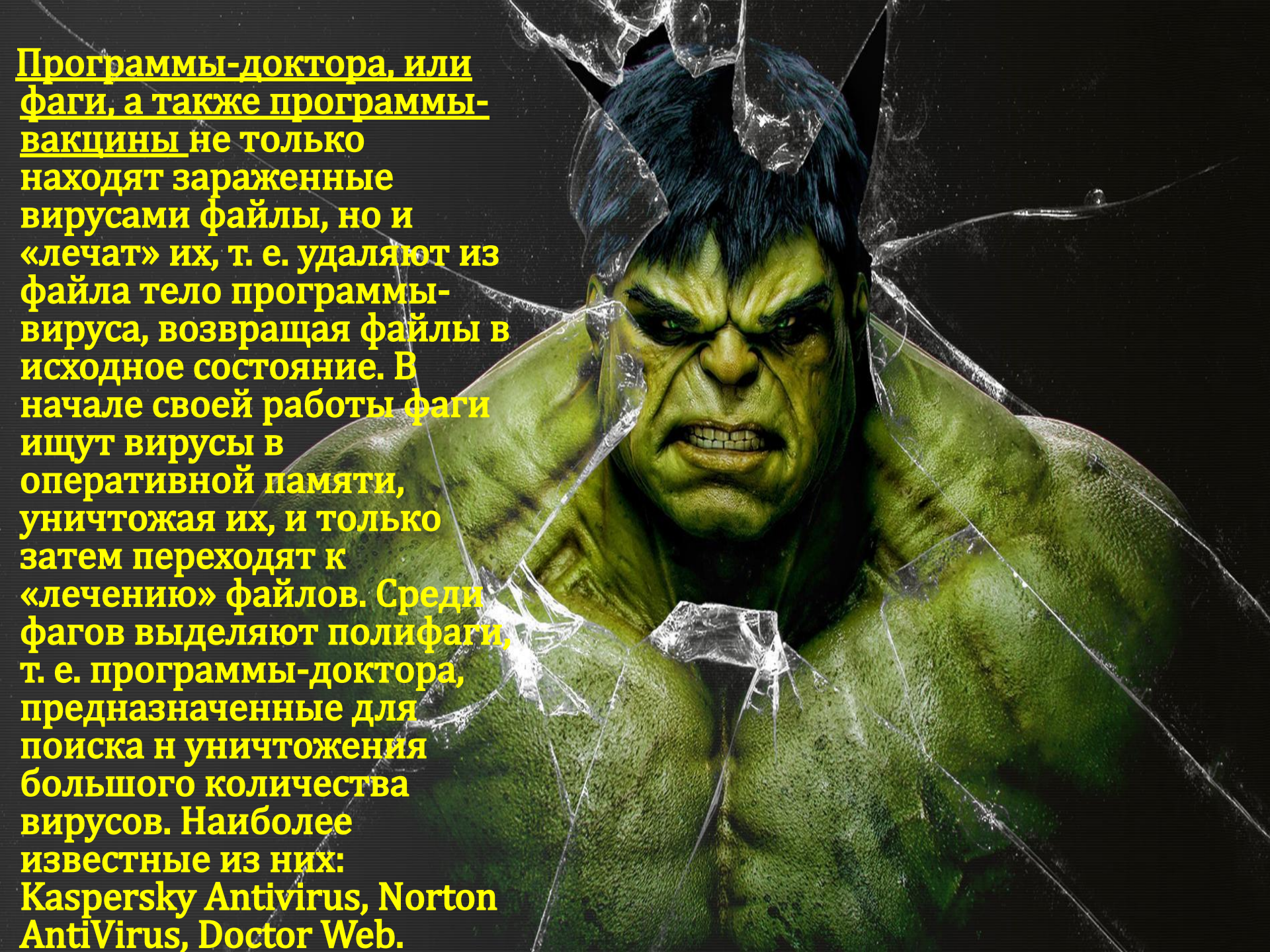
Первые антивирусные утилиты (1984 год) были написаны Анди Хопкинсом (Andy Hopkins). Программы CHK4BOMB и BOMBSQAD позволяли производить анализ загрузочного модуля с помощью контекстного поиска и перехватывать операции записи и форматирования, выполняемые через BIOS. На то время они были очень эффективны и быстро завоевали популярность.

Различают следующие
виды **антивирусных программ**:

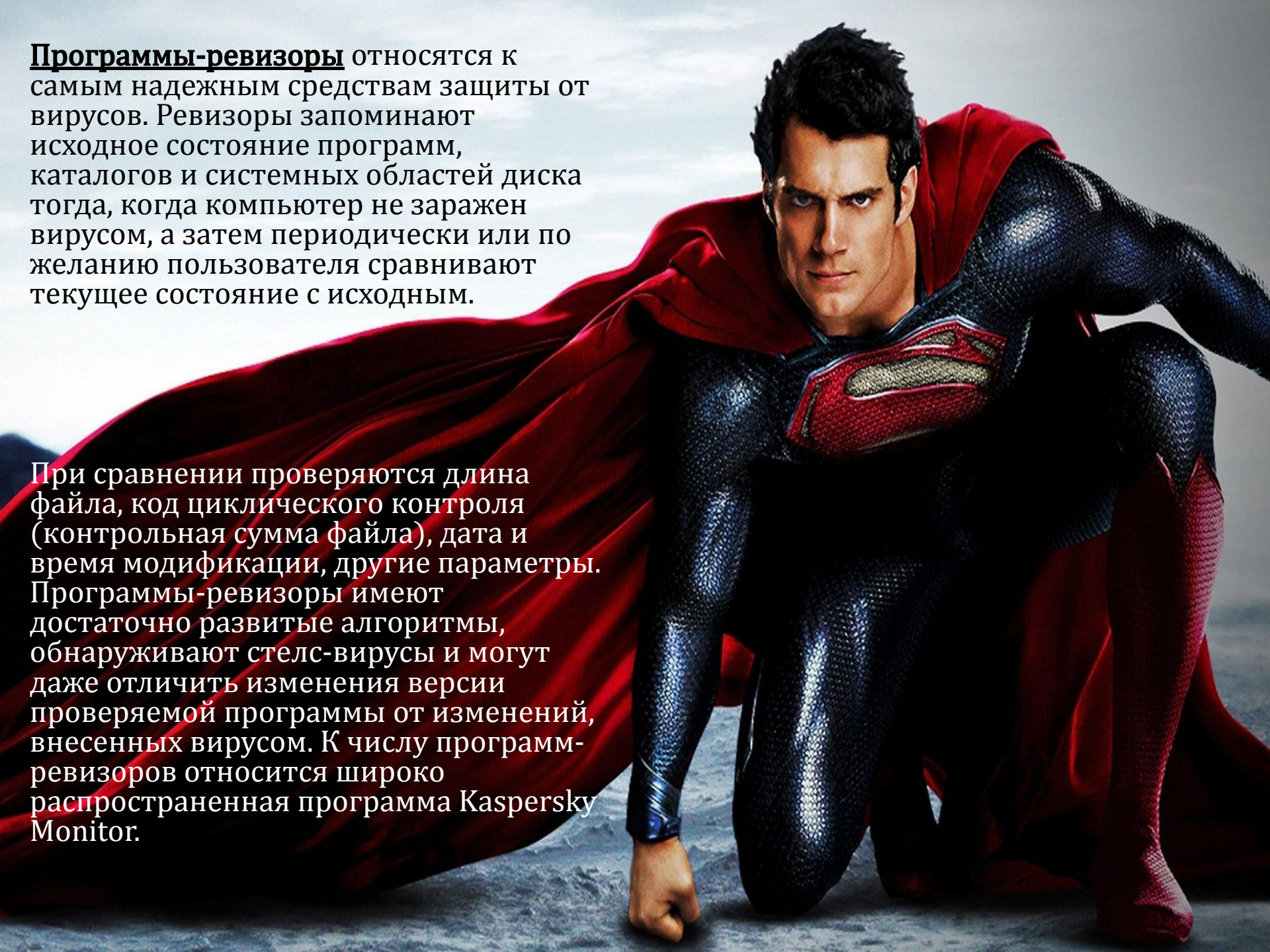
- программы-детекторы;
- программы-доктора, или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины, или иммунизаторы.



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, или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, т. е. 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, т. е. программы-доктора, предназначенные для поиска н уничтожения большого количества вирусов. Наиболее известные из них: Kaspersky Antivirus, Norton AntiVirus, Doctor Web.



Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры 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.

При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная программа Kaspersky Monitor.

Программы-фильтры 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;

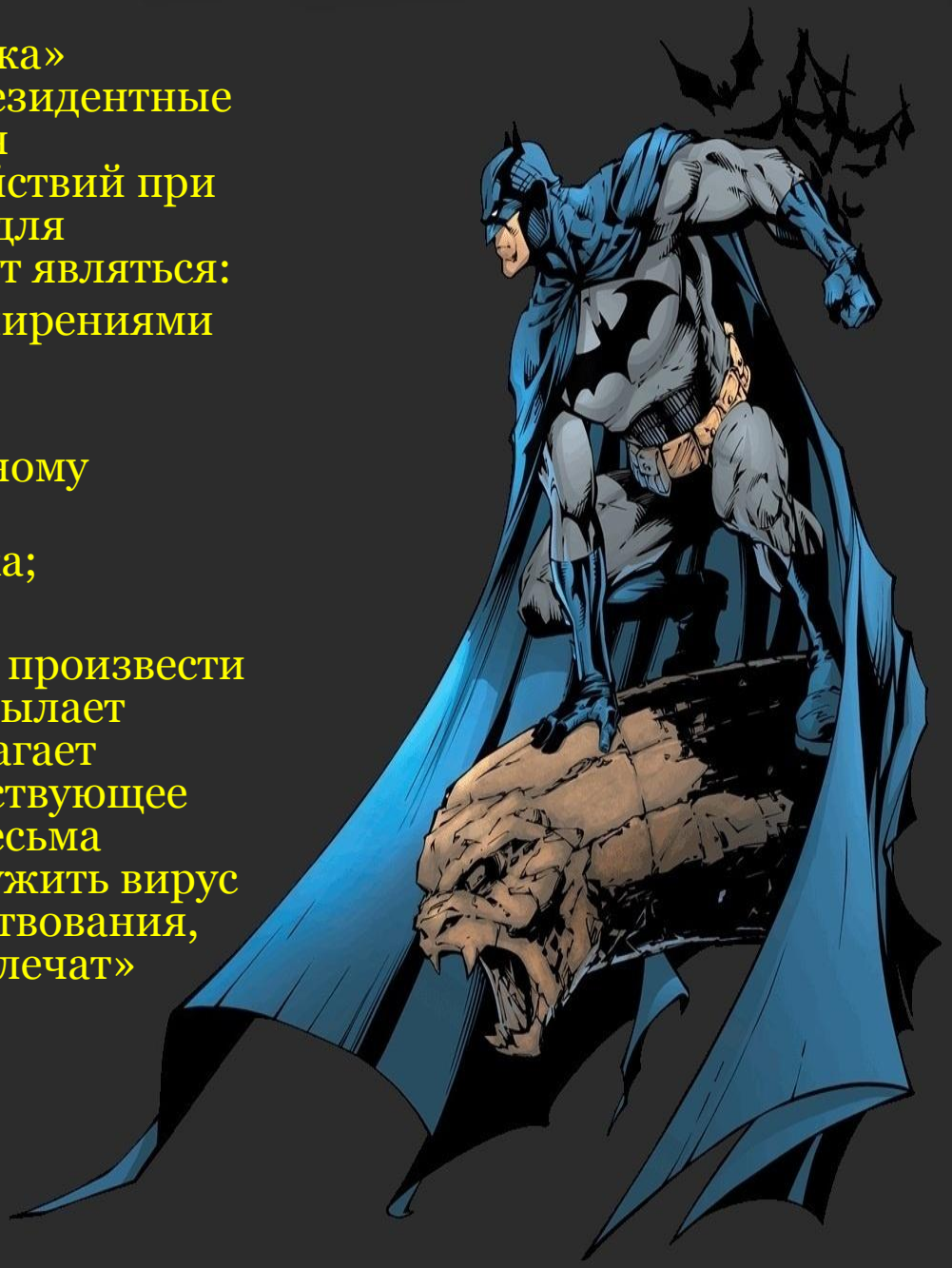
— изменение атрибутов файла;

— прямая запись на диск по абсолютному адресу;

— запись в загрузочные секторы 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.

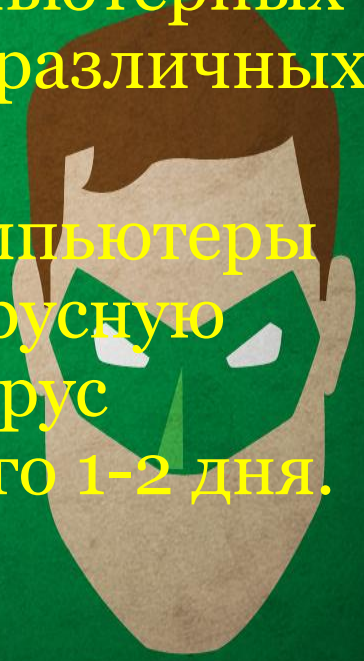


Вакцины или иммунизаторы — это резидентные программы. предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

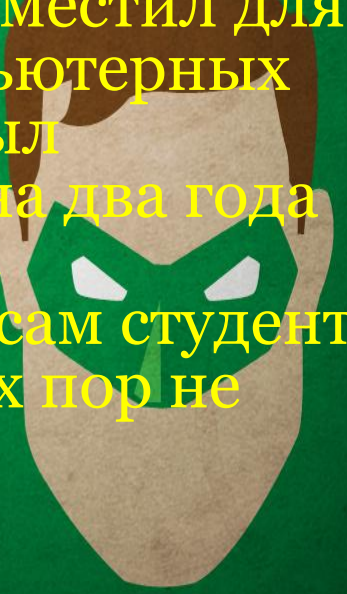
Интересные факты

- Каждый год проходит чемпионат мира по борьбе с вирусами. Несколько лет назад на этом чемпионате одержала победу россиянка, которая показала лучший результат. Она легко обезвредила 9600 вирусов из 10.000 возможных.
- По прогнозам специалистов Лаборатории Касперского, в этом году будут особенно активны и опасны вирусы, которые содержатся в Интернет - играх. В такие он-лайн игры лучше не играть на рабочем месте, если вам дорого содержание жёсткого диска.

- Сегодня в мире более 50 компаний-разработчиков антивирусного программного обеспечения. Более 5000 вирусологов по всему миру занимаются проблемами компьютерных вирусов. Изобретено уже более 300 различных антивирусных программ.
- Около 15% вирусов проникают в компьютеры несмотря на установленную антивирусную защиту. Ведь для того чтобы антивирус устарел, в наше время требуется всего 1-2 дня.



- Как говорит статистика, компьютерный вирус содержится в каждом 200-том электронном письме, которое отправляется в мире.
- Самый известный любитель вирусов в нашей стране – это студент одного из ВУЗов Воронежа. Он создал в Интернете сайт, на котором разместил для всех желающих целую коллекцию компьютерных вирусов (более 4.000 штук). Этот сайт был обнаружен ФСБ и студент был осужден на два года условно за распространение в интернете компьютерных вирусов. Что интересно, сам студент тоже написал свой вирус, который до сих пор не обнаруживается средствами защиты.



Спасибо за внимание☺️