1. Как антивирусы распознают так называемые "zip-бомбы"?

**Zip-бомба**, также известная как **Архив Смерти** или [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) ***decompression bomb*** — [архивный файл](https://ru.wikipedia.org/wiki/%D0%90%D1%80%D1%85%D0%B8%D0%B2_(%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)), который по своей природе обладает разрушающим действием. При распаковке может вызвать крах системы. Современные антивирусы вполне распознают подобные файлы и предупреждают пользователя о разрушающем действии. Внешне подобный файл выглядит как маленький архив. При распаковке распаковывается тот же самый архив. Данный файл может предоставлять опасность для [антивирусов](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81): в попытке распаковать все архивы антивирус может забить всю память и ничего не найти.

Лучше всего с ними бороться, устанавливая количество уровней декомпрессии для проверки антивирусом.

1. Нужно ли ставить антивирус на телефон? (Для разных ос)
2. Эффективны ли антивирусы для мобильных устройств?
3. Расскажите про антивирусы на мобильных устройствах, какие у них есть особенности?

В конце апреля 2013 эксперты компании Lookout Mobile Security обнаружили на Google Play тридцать две программы, содержащие инфицированную библиотеку. Вредоносный компонент был интегрирован под видом стандартной рекламной фукнции в игры, словари и утилиты уже после того, как они успешно прошли проверку в Google Play.

Всего заражённые программы были скачены около девяти миллионов раз. Помимо традиционных рекламных сообщений пользователи получали заведомо ложные предупреждения о мнимых угрозах и критических обновлениях. При клике на таком баннере происходило перенаправление на заражённый или фишинговый веб-сайт.

Скрыто от пользователя троянская компонента подключалась к контролируемым злоумышленниками удаленным серверам и передавали своим создателям собранную информацию, включая номер мобильного телефона и его IMEI. Дополнительно загружался троян семейства AlphaSMS, отправлявший SMS на платные номера.

Апрельский скандал получил продолжение. Недавно специалистами компании Webroot на Google Play был обнаружен очередной троян, распространяемый под видом программы управления шрифтами. Во всех случаях пострадавшие либо не пользовались антивирусами, либо последние оказались неэффективны.

В APP Store нет антивирусов.

1. Какие есть самые лучшие антивирусы для ос windows?
2. Kaspersky Internet Security 2015
3. Bitdefender Internet Security 2015
4. Qihoo 360 Internet Security (или 360 Total Security)
5. Антивирусы пол Linux.

Большинство разработчиков делают свои антивирусы и под Linux.

1. Платили ли вы когда-нибудь за антивирусы?

Нет.

1. Рейтинг использования антивирусов?

По количеству скачиваний с сайта Comss.ru за 2014:

1. [AVAST Software](http://www.comss.ru/page.php?al=AVAST_Software)
2. [Kaspersky Lab](http://www.comss.ru/dev/kaspersky.html)
3. [Doctor Web](http://www.comss.ru/dev/drweb.html)
4. [AVG Technologies](http://www.comss.ru/page.php?al=AVG_Technologies)
5. [ESET](http://www.comss.ru/dev/eset.html)
6. [Comodo](http://www.comss.ru/page.php?al=Comodo)
7. [Перфомикс/Adguard](http://www.comss.ru/page.php?id=1888)
8. [Qihoo 360](http://www.comss.ru/page.php?al=Qihoo_360)
9. [Avira Operations](http://www.comss.ru/page.php?al=Avira)
10. [Symantec/Norton](http://www.comss.ru/dev/symantec.html)
11. Как происходит карантин, лечение зараженного файла?

**Карантин** – это некоторая защищенная антивирусом область, которая позволяет понаблюдать за действиями файла, а также за работой программ и операционной системы в отсутствии этого файла на прежнем месте. Дело в том, что при перемещении файла в карантин он удаляется из своего первоначального месторасположения и копируется в некоторую папку, которая находится под контролем антивируса. Такой подход позволяет обезопасить себя от проблем, которые обязательно возникнут если вдруг какой-то важный для работы программы или операционной системы файл будет ошибочно удален антивирусом, ведь в случае возникновения проблем вы всегда сможете вернуть файл из карантина назад.

Чаще всего лечение доступно только при сигнатурном анализе. Из программы удаляется код вируса.

1. Существуют ли open source антивирусы ?

ClamAV.

1. Особенности panda anti-virus?

Panda Antivirus Pro 2012 (содержит: антивирус, антишпион, антифишинг, антируткит, файервол)

Panda Internet Security 2012 (содержит: антивирус, антишпион, антифишинг, антируткит, файервол, антиспам, родительский контроль). Panda Cloud Antivirus работает на основе Коллективного разума — системы, которая значительно увеличивает уровень обнаружения, не влияя на производительность компьютера.

1. Особенности Norton anti-virus? Почему он сейчас один из наиболее популярных?

**Norton Internet Security** (сокращенно NIS) — [пакет безопасности](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8), разработанный компанией [Symantec](https://ru.wikipedia.org/wiki/Symantec" \o "Symantec). Включает в себя [антивирус](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81), [брандмауэр](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD), сканер электронной почты, фильтр [спама](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC), защиту от фишинга. Существуют версии для [Windows](https://ru.wikipedia.org/wiki/Windows" \o "Windows) и [MAC](https://ru.wikipedia.org/wiki/Mac_OS).

Особенности:

1. Защищает от вирусов, программ-шпионов, вредоносных программ и прочих интернет-угроз
2. Защищает идентификационные данные и электронные транзакции
3. Предоставляет 100%-ную гарантию возврата денежных средств

Цена/Качество, интерфейс.

1. Какие из антивирусов являются наиболее эффективными, а какие наоборот лучше вообще не использовать?
2. Существуют ли какие-либо алгоритмы для выявления той или иной атаки?
3. Как вообще происходит выявление той или иной атаки?

Процесс обнаружения информационных атак (рис. 2) начинается со сбора исходных данных, необходимых для того, чтобы сделать вывод о проведении атаки в ИС. Примерами таких данных являются:

1. сведения о пакетах данных, передаваемых в ИС;
2. информация о производительности программно-аппаратного обеспечения ИС (вычислительная нагрузка на процессор хостов ИС, загруженность оперативной памяти, скорость работы прикладного ПО и др.);
3. сведения о доступе к файлам ИС;
4. информация о регистрации новых пользователей в ИС и др.

Информация, собранная сетевыми и хостовыми датчиками, анализируется СОА с целью выявления возможных атак нарушителей. Анализ данных может проводиться при помощи двух основных групп методов - сигнатурных и поведенческих.

1. В чем суть функции anti-work? Что она делает?

Возможно антивор.

Компонент **Анти-Вор** в **Kaspersky Internet Security для Android** предназначен для защиты хранящихся на устройстве данных от несанкционированного доступа к ним и поиска устройства в случае его кражи или потери.

С помощью **Анти-Вора** вы можете удаленно сделать следующее:

1. [Включить громкий сигнал тревоги (даже если звук был выключен) и заблокировать устройство](http://support.kaspersky.ru/10210).
2. [Определить местоположение устройства и заблокировать его](http://support.kaspersky.ru/10204).
3. [Удалить хранящуюся на устройстве информацию](http://support.kaspersky.ru/10207).
4. [Незаметно сделать фотографию человека, который сейчас использует ваше устройство](http://support.kaspersky.ru/10292).
5. [Узнать новый номер телефона и заблокировать устройство](http://support.kaspersky.ru/10206), если его включили с новой SIM-картой или вообще без нее.
6. Какой из антивирусов ты посоветуешь?
7. У Windows есть собственные средства борьбы с угрозами. Так что, востребованы ли сейчас антивирусы?
8. **Брандмауэр.**Брандмауэр защищает компьютер, предотвращая доступ к нему злоумышленников и вредоносных программ.
9. **Защита от вирусов.**Антивирусное программное обеспечение поможет защитить компьютер от вирусов, вирусов-червей и других угроз безопасности.
10. **Защита от шпионских и других вредоносных программ.** Антишпионское программное обеспечение поможет защитить компьютер от шпионских и других нежелательных программ.
11. **Центр обновления Windows.** Windows может регулярно проверять наличие обновлений для компьютера и автоматически их устанавливать.

Очевидно, что встроенные средства защиты Windows обеспечивают базовый уровень безопасности, которого должно быть достаточно для повседневной работы. Однако, если компьютер используется для осуществления более чувствительных с точки зрения безопасности действий, например, осуществления интернет-платежей, необходимо задуматься о более функционально наполненных решениях класса Internet Security. Кроме того, использование средств класса Internet Security оправдано, если компьютер используется дома и в семье есть маленькие дети — эти средства обладают более развитым и более гибким с точки зрения настроек модулей Родительского контроля.

1. Возможны ли ошибки в базах сигнатур? (Например, занесение невредоносного кода кода в базу.)

Наврятли.

1. Есть ли среди бесплатных антивирусов объективный лидер?

Объективно нет.

1. Почему Avast такой медленный?

Хз.

Сетевой экран тормозит.

1. Чем так хорош Касперский?

У каждого антивируса есть и плюсы и минусы.

Идеальных антивирусов нет, не было и не будет. Встречаются ли антивирусы со встроенным фаерволлом?

1. Стоит ли пользоваться антивирусом на Linux?

Лучший антивирус это благоразумие пользователя.

1. Как ведёт себя антивирус в случае заражения вирусом его исходных и рабочих файлов? Баз сигнатур?

Если антивирус имеет хорошую самозащиту, то его сложно сломать.

Он перестает правильно работать, может вообще перестать это делать, может удалиться.

1. Есть ли качественные оффлайн-антивирусы?

Не совсем понятно.

1. Каким образом разрабатывается вредоносное программное обеспечение? (вопрос слишком абстрактный, поэтому конкретизирую) Как разработать своего червя?
2. Войдите в систему как администратор.
3. **Откройте диск С:** и создайте там папку Programs.
4. **Откройте Блокнот и введите:** @echo off
5. **На второй строке введите:** Copy C:\Programs\virus.bat C:\Programs. На третьей строке введите: Start C:\Programs\virus.bat
6. **Нажмите «Сохранить как» и сохраните файл под именем virus.bat в созданной папке Programs.**
7. **Вставьте его ярлык в папку автозагрузки.**
8. **Вы успешно написали вирус (червь).** Чтобы запустить его, перезагрузите компьютер и на диске С: не останется свободного места.
9. Пробовали ли вы создавать вредоносное ПО?

Нет.

1. Как выстроена защита от вредоносного ПО на огромных серверах компаний-гигантов (Google, AWS)?

Хз.

1. Почему антивирус Касперского сильно тормозит всю систему, что он делает такого сложного?

Хз.

1. Какие файлы обновляются в антивирусе ESET, что входит в несколько килобайт его обновления и достаточно ли их ему для надёжной защиты компьютера?

Хз.

1. Когда стали появляться первые антивирусы?

Зимой 1984 г. Анди Хопкинс (Andy Hopkins) написал программы CHK4BOMB и BOMBSQAD. Первая из них 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. При выявлении запрещенной операции можно разрешить ее выполнение. В начале 1985 г. Ги Вонг (Gee Wong) написал программу DPROTECT - резидентную программу, перехватывающую попытки записи на дискеты и винчестер. Она блокировала все операции (запись, форматирование), выполняемые через BIOS. В случае выявления такой операции программа требует рестарта системы. Несколько позднее появилась программа FLUSHOT, написанная Росс М. Гринберг. Более поздняя версия этой программы - FluShot Plus (версия 1.7), распространяемая как SHAREWARE с регистрационной ценой 10 долларов, используется и в настоящее время.

1. Можно ли утверждать, что вирусы пишутся специально, чтобы потом продавать для них антивирусы?

Наврятли.

1. Может ли компьютер нормально функционировать без антивируса, если нет подключения к интернету?

В принципе, не считая флеш вирусов, да.

1. Как и кем осуществляется поддержка словаря сигнатур?

В антивирусных компаниях

1. Какой из методов защиты наиболее успешен/популярен?

Комбинированный.

1. Какие мат. методы участвуют в анализе кода? Можно ли говорить о высокой эффективности этих методов?

Антивирус просматривает код программы и находит соответствие сигнатур вирусов.

Это очень эффективно, т.к. вероятность ошибки крайне мала.

1. Как распознается новый вирус? Обратная связь?

Эвристический анализ.

1. Правда, что качество антивируса прямо пропорционально кол-ву потребляемых им ресурсов?

Нет.