ЛЕКЦИЯ

«АНТИВИРУСНАЯ ЗАЩИТА КОМПЬЮТЕРА»

ВОПРОСЫ ЛЕКЦИИ

1. Компьютерные вирусы.
2. Фишинг и фарминг.
3. Как защититься от вредоносного ПО.
4. Методы обнаружения вирусов.
5. Антивирусные программы.

ЛИТЕРАТУРА:

1. К.Е. Климентьев. Компьютерные вирусы и антивирусы. Взгляд программиста. – М.: ДМК Пресс, 2015. – 656 с.

2. А.В. Михайлов. Компьютерные вирусы и борьба с ними. – М.: Диалог-МИФИ, 2011. – 104 с.

3. С.Н. Никифоров. Методы защиты информации. Защита от внешних вторжений. Учебное пособие. – СПб.: Лань, 2018. – 96 с.

4. Валентин Холмогоров. Pro Вирусы. – М.: Страта, 2015. – 142 с.

5. Вирусная энциклопедия «Лаборатории Касперского» [электронный ресурс]. URL: https://encyclopedia.kaspersky.ru (Дата обращения: 14.02.2020).

1. Компьютерные вирусы

Компьютерные вирусы не зря так названы – их сходство с «живыми» вирусами поражает. Они так же распространяются, живут, действуют, так же умирают. Разница лишь в том, что в качестве мишени выступают не люди и не животные, а компьютеры. Контактируя между собой посредством физических носителей информации и локальных сетей, Интернет и других средств «общения», они, как и человек, заражают друг друга.

Компьютерным вирусом называется программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и

внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения. Программа, внутри которой находится вирус, называется зараженной (инфицированной) программой.

Когда инфицированная программа начинает работу, то сначала управление получает вирус. Он заражает другие программы, а также выполняет запланированные деструктивные действия. Для маскировки своих действий вирус активизируется не всегда, а лишь при выполнении определенных условий (истечение некоторого времени, выполнение определенного числа операций, наступление некоторой даты или дня недели и т.д.). После того, как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится. Внешне зараженная программа может работать так же, как и обычная программа. Подобно настоящим вирусам компьютерные вирусы прячутся, размножаются и ищут возможности перейти на другие электронные устройства.

Типы вредоносного ПО

Вредоносные программы ведут себя по-разному. Одни могут скрываться во вложениях электронной почты или использовать веб-камеру вашего устройства, чтобы шпионить за вами. Другие (программы-вымогатели) могут удерживают ваши файлы в качестве заложников, пока вы не заплатите выкуп.

Существует несколько разновидностей вредоносных программ. Давайте рассмотрим поведение некоторых из них, чтобы вы смогли понять природу угроз, представляющих опасность для вашего устройства. Начнем с основных определений.

Вирус

Вирус - это тип вредоносного ПО, способный к самовоспроизведению и распространению по всей системе на вашем устройстве.

Черви

Червь – это вредоносная программа, которая многократно копирует сама себя, но не наносит прямого вреда безопасности. Черви могут распространяться по сетям, используя уязвимости каждого устройства.

Как и другие виды вредоносного ПО, червь может нанести вред вашему устройству, загружая на него вредоносные программы и замусоривая канал связи.

Черви — как уже говорилось, вредоносные программы, которые для распространения используют сетевые ресурсы. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы.

Черви обладают очень высокой скоростью распространения. Они проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Черви также могут использовать данные адресной книги почтовых клиентов.

Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера за исключением оперативной памяти. Скорость распространения червей выше, чем у вирусов.

Большинство известных компьютерных червей распространяется следующими способами:

- в виде файла, отправленного во вложении в электронном письме;
- в виде ссылки на интернет - или FTP-ресурс;
- в виде ссылки, переданной через сообщение мессенджера;
- через пиринговые сети обмена данными P2P (peer-to-peer);
- некоторые черви распространяются как сетевые пакеты. Они проникают прямо в компьютерную память, затем активируется код червя.

Компьютерные черви могут использовать ошибки конфигурации сети (например, чтобы скопировать себя на полностью доступный диск) или

бреши в защите операционной системы и приложений. Многие черви распространяют свои копии через сеть несколькими способами.

Adware

Adware — это программы, которые предназначены для показа рекламы на вашем компьютере, часто в виде всплывающих окон. Вы можете случайно согласиться на просмотр какого-то рекламного объявления и таким образом загрузить нежелательное ПО.

Иногда хакеры встраивают шпионское ПО в Adware, и тогда оно становится особенно опасным, поэтому будьте внимательны, не нажимаете на рекламное объявление, которое выглядит подозрительно. С другой стороны, иногда подобные вредоносные программы не являются шпионскими, т.к. собирают данные о пользователе с его ведома и разрешения.

Riskware

Riskware – программы, которые могут уничтожить, заблокировать, изменить или скопировать данные, нарушить работу компьютера.

К таким программам относятся:

- коммерческие утилиты удаленного администрирования;
- программы-клиенты IRC;
- программы дозвона;
- программы для загрузки файлов;
- мониторы активности компьютерных систем;
- утилиты для работы с паролями;
- интернет-серверы служб FTP, Web, Proxy и Telnet.

Троянские программы

Троянская программа или троян - это вредоносная программа, маскирующаяся под обычный файл и выполняющая на компьютере пользователя вредоносные действия. При загрузке трояна сам пользователь может даже не подозревать, что на самом деле устанавливаете вредоносное

ПО. Троянские программы могут выполнять различные действия, включая кражу персональных данных.

Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина, то есть не заражает другие программы или данные. Троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом наносимый ими вред может во много раз превышать потери от традиционной вирусной атаки.

Шпионское ПО

Шпионское ПО отличается от других типов вредоносных программ тем, что это не техническое определение, а общий термин для Adware, Riskware и троянских программ. Шпионское ПО отслеживает вашу активность в интернете, наблюдает за тем, какие клавиши вы нажимаете, и собирает ваши личные данные без вашего ведома.

Боты

Боты создаются автоматически для выполнения специальных операций. Некоторые боты создаются для выполнения вполне легитимных задач. Например, они могут использоваться для сканирования веб-сайтов и сбора их контента с целью занесения этой информации в поисковые системы.

При злонамеренном использовании боты могут искать и собирать личные данные и передавать их киберпреступникам.

Программы-вымогатели

Программы-вымогатели блокируют доступ к вашему устройству или шифруют информацию, которая хранится на нем, а затем требуют плату за расшифровку файлов и восстановление работы системы.

Руткиты

Руткиты — это программы, используемые хакерами для предотвращения обнаружения при попытке получить несанкционированный

доступ к компьютеру. Хакеры используют руткиты для удаленного доступа и кражи вашей информации.

- **Дро́ппперы:** Эти программы используются хакерами, чтобы скрытно устанавливать вредоносные программы на компьютеры пользователей.
- **Троянские программы скрытой загрузки:** Эти программы способны загружать и устанавливать на компьютер-жертву новые версии вредоносных программ.
- **Шпионские программы:** Эти программы способны скрытно наблюдать за вашей активностью в интернете и отправлять информацию о ней киберпреступникам.
- **Банковские троянцы:** Эти программы маскируются под легитимные приложения и крадут банковскую информацию, когда вы их загружаете.
- **Бэкдоры:** Эти вредоносные программы скрытно проникают в ваш компьютер, используя уязвимости в установленном на нем программном обеспечении.

Многофункциональные вредоносные программы

Отдельные вредоносные программы часто выполняют несколько вредоносных функций и используют несколько способов распространения. Без некоторых дополнительных правил классификации это могло бы привести к путанице

Например. Существует вредоносная программа, которая занимается сбором адресов электронной почты на зараженном компьютере без ведома пользователя. При этом она распространяется как в виде вложений электронной почты, так и в виде файлов через сети P2P.

Тогда программу можно классифицировать и как Email-Worm, и как P2P-Worm или Trojan-Mailfinder. Чтобы избежать такой путаницы, применяется набор правил, которые позволяют однозначно классифицировать вредоносную программу по конкретному поведению, независимо от второстепенных свойств:

- Если вредоносная программа имеет несколько функций с одинаковым уровнем опасности (таких как Trojan-Ransom, Trojan-ArcBomb, Trojan-Clicker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper, Trojan-IM, Trojan-Notifier, Trojan-Proxy, Trojan-SMS, Trojan-Spy, Trojan-Mailfinder, Trojan-GameThief, Trojan-PSW or Trojan-Banker), она классифицируется как троянская программа.
- Если у вредоносной программы есть несколько функций с одинаковым уровнем опасности, таких как IM-Worm, P2P-Worm или IRC-Worm, она классифицируется как червь.

2. Фишинг и фарминг

Теперь рассмотрим некоторые разновидности интернет-мошенничества. В первую очередь, наверное, следует назвать фишинг — вид интернет-мошенничества, целью которого является получение доступа к логинам и паролям пользователей. Фишинг (англ. phishing, от *fishing* — рыбная ловля, выуживание и *password* — пароль) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Для получения пользовательских данных злоумышленник создает точную копию сайта интернет-банка и составляет сообщение, максимально похожее на настоящее письмо от выбранного банка. В нем злоумышленник под видом сотрудника банка просит пользователя подтвердить или изменить свои учетные данные и приводит ссылку на поддельный сайт интернет-банка. Цель такого письма — заставить пользователя нажать на приведенную ссылку и ввести свои данные.

Технологии фишеров совершенствуются. Так, появилось сопряженное с фишингом понятие — фарминг. Это тоже мошенничество, ставящее целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNS

цифровые адреса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опасней, так как заметить подделку практически невозможно.

Наиболее популярные фишерские мишени — аукцион Ebay и платежная система PayPal. Также страдают различные банки по всему миру. Атаки фишеров бывают случайными и целевыми. В первом случае атака производится «наобум». Атакуются наиболее крупные и популярные объекты — такие как аукцион Ebay — так как вероятность того, что случайный получатель имеет там учетную запись, довольно высока. Во втором случае мошенники узнают, каким именно банком, платежной системой, провайдером, сайтом пользуется адресат. Этот способ более сложен и затратен для фишеров, зато больше шансов, что жертва купится на провокацию.

Воровство конфиденциальных данных — не единственная опасность, поджидающая пользователя при нажатии на фишерскую ссылку. Зачастую, следуя по ней, можно получить программу-шпиона, кейлоггер или троян. Так что если даже у вас нет счета, которым мошенники могли бы воспользоваться, нельзя чувствовать себя в полной безопасности.

Успеху фишинг-афер способствует низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. И хотя на многих сайтах, требующих конфиденциальной информации, опубликованы специальные предупреждения о том, что они никогда не просят сообщать свои конфиденциальные данные, пользователи продолжают слать свои пароли мошенникам.

Для борьбы с этим явлением была создана Anti-Phishing Working Group (APWG) — группа по борьбе с фишингом, в которую входят как компании-«мишени» фишеров, так и компании, разрабатывающие анти-фишинговый/анти-спамерский софт. В рамках деятельности APWG проводятся ознакомительные мероприятия для пользователей, также члены

APWG информируют друг друга о новых фишерских сайтах и угрозах. Сейчас APWG насчитывает тысячи участников, среди которых есть крупнейшие мировые банки и ведущие IT-компании. Так что, по оптимистическим прогнозам, через некоторое время пользователи научатся остерегаться фишерских сайтов, как в свое время научились с опаской относиться к письмам с вложениями от неизвестных адресатов. Пока же основной защитой от фишинга остаются спам-фильтры.

Спам — это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга. Долгое время спам в огромных количествах рассылался по электронной почте спамерами и киберпреступниками, цель которых:

- выудить деньги у некоторого количества получателей, ответивших на сообщение;
- провести фишинговую атаку, чтобы обманным путем получить пароли, номера кредитных карт, банковские учетные данные и т.д.;
- распространить вредоносный код на компьютерах получателей.

Более подробную информацию по защите от спама и фишинга смотрите на сайте «Лаборатории Касперского».

3. Как защититься от вредоносного ПО

В условиях, когда вредоносное ПО становится все более совершенным, а мы все больше своих личных данных храним в Интернете, угроза того, что вредоносные программы украдут нашу конфиденциальную информацию и используют ее в мошеннических целях, является более чем реальной.

Есть несколько способов защитить себя. Первое и главное правило - использование антивирусной защиты. Следуйте приведенным ниже рекомендациям, они помогут предотвратить заражение ваших устройств вредоносными программами и не дать им возможности получить доступ к вашей личной информации.

Скачивайте приложения только с доверенных сайтов

Чтобы снизить риск заражения вредоносным ПО, скачивайте приложения, программное обеспечение или мультимедийные файлы только с доверенных сайтов. Пользуйтесь Google Play Store на Android или App Store для iPhone. Помните: загружая файлы или приложения с незнакомых сайтов, вы, скорее всего, загрузите и вредоносное ПО, даже не подозревая об этом.

Проверяйте описания разработчиков

Хотя и редко, но бывает, что вредоносное ПО из сети попадает на сайты, пользующиеся хорошей репутацией. Поэтому всегда читайте информацию о разработчике в описании. Вам известен этот девелопер? Нет - поищите отзывы о нем в Google. Ничего не нашли - в целях безопасности не скачивайте файлы с этого сайта.

Читайте отзывы пользователей

Обязательно читайте отзывы пользователей о любом ПО или приложениях, которые вы собираетесь скачать. Они выглядят достоверными? Хакеры, пытающиеся побудить пользователей загружать вредоносные программы, могут подделывать отзывы, поэтому следует быть внимательным и проверять все, что выглядит подозрительным.

Сигналом тревоги для вас должны стать только положительные отзывы о приложении или программе: как правило, в настоящих отзывах отмечаются как положительные, так и отрицательные аспекты приложения.

Проверяйте количество скачиваний

Приложения, зараженные вредоносным ПО, вряд ли будут иметь тысячи скачиваний, тогда как приложения с миллионами загрузок с меньшей долей вероятности являются вредоносными. Если приложение популярно (с большим количеством отзывов и загрузок), можно не беспокоиться - риск того, что оно вредоносное, будет значительно ниже.

Проверяйте запрашиваемые разрешения

Посмотрите, какие разрешения требует от вас приложение или программное обеспечение. Запрашиваемые разрешения кажутся вам

разумными? Если вы считаете, что запрашиваемые разрешения не являются необходимым для работы приложения или программы, будьте осторожны – не скачивайте приложение или удалите его, если вы его уже установили.

Не нажимайте на непроверенные ссылки

Не нажимайте на непроверенные ссылки в спам-рассылках, сообщениях или на подозрительно выглядящих веб-сайтах. Нажатие на зараженную ссылку может автоматически запустить загрузку вредоносного ПО.

Помните, что ваш банк никогда не попросит вас отправить им ваше имя пользователя и пароль. Если вы получили сообщение с подобной просьбой, не открывайте его, не передавайте свою информацию (даже если оно выглядит легитимным) и немедленно свяжитесь с банком, чтобы перепроверить информацию.

Регулярно обновляйте операционную систему и приложения

Регулярное обновление операционной системы важно для защиты от вредоносных программ. Это означает, что ваше устройство использует последние обновления безопасности.

Важно так же регулярно обновлять приложения на ваших устройствах. Это позволяет разработчику приложения или программного обеспечения исправлять любые обновления безопасности, чтобы защитить ваши устройства и данные.

Не игнорируйте это правило: хакеры и вредоносные программы как раз и рассчитывают на то, что вы не обновите свои приложения, и тем самым дадите им возможность использовать лазейки в программном обеспечении для получения доступа к вашим устройствам.

Будьте внимательны при пользовании бесплатным Wi-Fi

Если вы пользуетесь ноутбуком или смартфоном в кафе или общественных местах, будьте осторожны с бесплатным Wi-Fi. Не вводите конфиденциальные данные на сайтах интернет-магазинов или для совершения банковских операций. Если вам нужно подключится по

бесплатному Wi-Fi, используйте VPN-соединение, например, Kaspersky Secure Connection: оно защищает ваше соединение путем шифрования ваших данных.

Никогда не пользуйтесь чужими USB-устройствами

Никогда не вставляйте чужое USB-устройство в свой ноутбук или настольный компьютер – оно может быть заражено вредоносным ПО.

Ваше устройство заражено?

Ваш ноутбук, настольный компьютер или смартфон ведут себя странно? Большинство вредоносных программ ненавязчивы и не видны невооруженным глазом. Однако есть некоторые предупреждающие знаки, указывающие на то, что ваше устройство может быть заражено вредоносным ПО.

Для диагностики заражения вредоносным ПО обратите внимание на следующие предупреждающие знаки:

- Ваше устройство стало работать медленнее, и все операции занимают больше времени.
- Появились приложения или программы, о которых вы ничего не знаете.
- Приложения или программы постоянно «слетают» без видимой причины.
- Сетевой трафик на вашем смартфоне необъяснимо возрос.
- Ваш телефонный счет таинственным образом увеличился.
- Вы видите всплывающие окна, когда ваш браузер закрыт.
- Батарея вашего телефона быстро разряжается.
- Ваш ноутбук, настольный компьютер или смартфон перегреваются.

Удаление вредоносной программы

Если вы считаете, что ваш ноутбук, настольный компьютер или смартфон заражен, необходимо немедленно принять меры по удалению вредоносного ПО.

4. Методы обнаружения вирусов

Назовем основные методы поиска и обнаружения компьютерных вирусов:

1) Метод соответствия определению вирусов в словаре.

Это метод, когда антивирусная программа, просматривая файл, обращается к антивирусным базам, которые составлены производителем программы-антивируса. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в базах, программа антивирус может по запросу выполнить одно из следующих действий:

- Удалить инфицированный файл.
- Заблокировать доступ к инфицированному файлу.
- Отправить файл в карантин (то есть сделать его недоступным для выполнения с целью недопущения дальнейшего распространения вируса).
- Попытаться восстановить файл, удалив сам вирус из тела файла.
- В случае невозможности лечения/удаления, выполнить эту процедуру при перезагрузке.

Для того чтобы такая антивирусная программа успешно работала на протяжении долгого времени, в словарь вирусов нужно периодически загружать (обычно, через Интернет) обновленные данные.

Для многих антивирусных программ со словарем характерна проверка файлов в тот момент, когда операционная система создает, открывает, закрывает или посылает их по почте. Таким образом, программа может обнаружить известный вирус сразу после его первого попадания в компьютер. Заметьте также, что системный администратор может установить в антивирусной программе расписание для регулярной проверки (сканирования) всех файлов на жестком диске компьютера. Хотя антивирусные программы, созданные на основе поиска соответствия определению вируса в словаре, при обычных обстоятельствах могут достаточно эффективно препятствовать вспышкам заражения компьютеров,

авторы вирусов стараются держаться на полшага впереди таких программ-антивирусов, создавая «олигоморфические», «полиморфические» и «метаморфические» вирусы, в которых некоторые части шифруются или искажаются так, чтобы было невозможно обнаружить совпадение с определением в словаре вирусов.

2) Метод обнаружения странного поведения программ.

Антивирусы, использующие метод обнаружения подозрительного поведения программ, не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается записать какие-то данные в исполняемый файл (exe-файл), программа-антивирус может пометить этот файл, предупредить пользователя и спросить, что следует сделать. В настоящее время, подобные превентивные методы обнаружения вредоносного кода, в том или ином виде, широко применяются в качестве модуля антивирусной программы, а не отдельного продукта. Другие названия: Проактивная защита, Поведенческий блокиратор, Host Intrusion Prevention System (HIPS).

В отличие от метода поиска соответствия определению вируса в антивирусных базах, метод обнаружения подозрительного поведения даёт защиту от новых вирусов, которых ещё нет в антивирусных базах. Однако следует учитывать, что программы или модули, построенные на этом методе, выдают также большое количество предупреждений (в некоторых режимах работы), что делает пользователя мало восприимчивым ко всем предупреждениям. В последнее время эта проблема ещё более ухудшилась, так как стало появляться всё больше не вредоносных программ, модифицирующих другие exe-файлы, несмотря на существующую проблему ошибочных предупреждений. Несмотря на наличие большого количества предупреждающих диалогов, в современном антивирусном программном обеспечении этот метод используется всё больше и больше.

Так, еще в 2006 году вышло несколько продуктов, впервые реализовавших этот метод, например, Kaspersky Internet Security. Многие

программы класса файрвол издавна имели в своем составе модуль обнаружения странного поведения программ.

3) Метод обнаружения при помощи эмуляции.

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет себя как вирус (например, немедленно начинает искать другие exe-файлы), такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

4) Метод «Белого списка».

Общая технология по борьбе с вредоносными программами — это «белый список». Вместо того, чтобы искать только известные вредоносные программы, это технология предотвращает выполнение всех компьютерных кодов за исключением тех, которые были ранее обозначены системным администратором как безопасные. Выбрав этот параметр отказа по умолчанию, можно избежать ограничений, характерных для обновления сигнатур вирусов. К тому же, те приложения на компьютере, которые системный администратор не хочет устанавливать, не выполняются, так как их нет в «белом списке». Так как у современных предприятий есть множество надежных приложений, ответственность за ограничения в использовании этой технологии возлагается на системных администраторов и соответствующим образом составленные ими «белые списки» надежных приложений. Работа антивирусных программ с такой технологией включает инструменты для автоматизации перечня и эксплуатации действий с «белым списком».

Кроме названных имеется и ряд других методов, которые используется в антивирусных программах.

5. Антивирусные программы

Для борьбы с вирусами созданы специальные антивирусные программы, позволяющие выявлять вирусы, лечить заражённые файлы, обнаруживать и предотвращать подозрительные (характерные для вирусов) действия. Разумеется, антивирусные программы надо применять наряду с регулярным резервированием данных и использованием профилактических мер, позволяющих уменьшить вероятность заражения вирусом.

При работе с антивирусными программами необходимо знать некоторые понятия:

Ложное срабатывание – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

Пропуск вируса – не детектирование вируса в зараженном объекте.

Сканирование по запросу – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

Сканирование налету – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.).

В работе антивирусов, как следует из вышеизложенного, можно выделить три составляющих:

1.Диагностика.

Антивирус проверяет все доступные для вирусов места на жёстком диске компьютера, и если он обнаруживает вирус, то оповещает об этом пользователя компьютера.

2.Лечение.

Найдя вирус, антивирусная программа может (по усмотрению пользователя):

- Попытаться вылечить заражённый файл.
- Поместить его в карантин. То есть, если этот файл ценен для вас и содержит какую-то важную информацию, его можно поместить в папку

карантина. В дальнейшем, вы можете попытаться его вылечить “вручную” самостоятельно либо же с помощью специалиста, иногда это помогает.

- Удалить инфицированный файл. Если лечение файла оказалось невозможным, он либо безнадёжно испорчен вирусом, либо он сам является вирусом. Значит такой файл необходимо просто удалить с компьютера.

- Вы можете не предпринимать никаких действий. Иногда антивирус выдаёт ложную тревогу и если вы уверены, что просканированный файл не является вирусом, то вы смело можете дать отбой своему антивирусу.

3.Профилактика.

Полноценные антивирусные программы, как правило, действуют/защищают компьютер всё время (постоянно). То есть, запускаются вместе с запуском операционной системы и проверяют на наличие вирусов каждую запускаемую программу (файл) и если она содержит вирус или вызывает какое-либо подозрение, то антивирус сразу же даёт вам об этом знать, и далее предлагает вам на выбор принять решение что с этой программой необходимо сделать: вылечить или поместить в карантин, удалить её с компьютера, либо продолжить работу, не предпринимая никаких действий по отношению к данному файлу.

Принцип работы компьютерных антивирусов:

Во-первых, каждый компьютерный антивирус содержит антивирусную базу данных, то есть он знает все имеющиеся в наличии на сегодняшний день вирусы (почти все) поимённо, можно сказать “в лицо”. “Лицо” этих вирусов – это так называемая сигнатура, то есть признаки по которым их можно определить.

При работе антивируса (проверке файлов), антивирус сверяет все сканируемые им файлы по своей базе данных и если обнаруживается подозрительный файл, то он сразу срабатывает и “бьёт” тревогу.

Антивирусная база обновляется. Обновляется она очень часто, иногда даже по несколько раз в день, потому что каждый день появляется очень

много новых вирусов; которые, соответственно, и заносятся в антивирусную базу.

Второе, эвристическая методика определения вирусов, то есть, антивирус анализирует программу, если он видит какой-либо подозрительный, по его мнению, участок кода, то он тоже вас предупреждает об этом, но тут, конечно, невозможно дать 100%-ные гарантии, что та или иная подозрительная программа — это обязательно вирус, поэтому могут быть и ошибки, но всё-таки очень часто такие подозрительные программы, впоследствии, действительно оказываются вредоносными.

Ну и, напоследок, конечно, необходимо упомянуть о том, что в антивирусных программах, как правило, предусмотрено несколько режимов проверки на наличие вирусов.

Обычно их бывает три:

1) Максимальный уровень защиты. Всё включено по полной, эвристические алгоритмы включены на полную мощность.

Максимальный режим обеспечивает максимальную степень защиты, но обычно при этом потребляя значительное количество ресурсов компьютера. При данном режиме работа компьютера (быстродействие) существенно замедляется, так же при сканировании бывает много ложных срабатываний.

2) Средний уровень защиты (**оптимальный**). Он не слишком замедляет работу компьютера и, в то же время, обеспечивает достаточный уровень защиты, он рекомендуется для повседневной работы. Обычно рекомендуется разработчиками антивирусных программ как по умолчанию.

3) Минимальный уровень защиты. Обычно включает в себя проверку по базе данных, то есть антивирус выдаёт вам информацию только если перед вами действительно 100% вирус.

Виды антивирусных программ:

- Программы-детекторы (сканеры) – рассчитаны на обнаружение конкретных вирусов. Основаны на сравнении характерной (специфической) последовательности байтов (сигнатур или масок вирусов), содержащихся в

теле вируса, с байтами проверяемых программ. Эти программы нужно регулярно обновлять, т.к. они быстро устаревают и не могут выявлять новые виды вирусов. Если программа не опознается детектором как зараженная, это еще не значит, что она «здорова». В ней может быть вирус, который не занесен в базу данных детектора.

- Программы-доктора (фаги, дезинфекторы) – не только находят файлы, зараженные вирусом, но и лечат их, удаляя из файла тело программы-вируса. Полифаги – позволяют лечить большое число вирусов. Широко распространены программы-детекторы, одновременно выполняющие и функции программ-докторов.

- Программы-ревизоры – анализируют текущее состояние файлов и системных областей дисков и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние Boot-сектора, FAT, а также длина файлов, их время создания, атрибуты, контрольные суммы (суммирование по модулю 2 всех байтов файла). Программы-ревизоры являются наиболее надежными в плане защиты от вирусов.

- Программы-мониторы (файерволы, брандмауэры) начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас". Программы-фильтры – резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия, а пользователь принимает решение о разрешении или запрещении выполнения этих действий. Фильтры контролируют следующие операции: обновление программных файлов и системной области дисков; форматирование диска; резидентное размещение программ в ОЗУ.

- Программы-иммунизаторы – это программы записывающие в другие программы коды, сообщающие о заражении. Они обычно записывают эти коды в конец файлов (по принципу файлового вируса) и при запуске файла

каждый раз проверяют его на изменение. Недостаток у них всего один, но он летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время. Кроме того, многие программы сами проверяют себя на целостность и могут принять внедренные в них коды за вирусы и отказаться работать.

Рассмотрим для примера одну из наиболее популярных антивирусных программ.

Kaspersky Internet Security 7.0. Программа для комплексной защиты ПК от вирусов и всех других типов вредоносных программ, а также от хакерских атак и спама. Обеспечивает удобную и безопасную работу в глобальной интернет-среде.

Антивирус Касперского 7.0. Классическая защита компьютера от вирусов, троянских и шпионских программ, а также от любого другого вредоносного ПО. Решение эффективно противостоит как известным, так и новым вредоносным программам.

Преимущества Антивируса Касперского заключаются в следующем:

- Интегрированная защита от всех Интернет-угроз;
- Комплексная антивирусная защита:
    1. проверка по базам сигнатур;
    2. эвристический анализатор;
    3. поведенческий блокиратор.
- Проверка файлов, почты и интернет-трафика в режиме реального времени.
- Персональный сетевой экран с системой IDS/IP.
- Предотвращение утечек конфиденциальной информации.
- Родительский контроль.
- Защита от спама и фишинга.
- Автоматическое обновление баз.

Основные функции Антивируса Касперского:

- Защита от вирусов, троянских программ и червей.
- Защита от шпионского (spyware) и рекламного (adware) программного обеспечения (ПО).
- Проверка файлов, почты и интернет-трафика в режиме реального времени.
- Защита от вирусов при работе с ICQ и другими IM-клиентами.
- Защита от всех типов клавиатурных шпионов.
- Обнаружение всех видов руткитов.
- Отмена нежелательных изменений на вашем компьютере.
- Средства создания диска аварийного восстановления системы.
- Автоматическое обновление баз.
- Бесплатная техническая поддержка.

Защита Антивируса Касперского от вирусов является комплексной и включает в себя:

- Защиту электронной почты. Антивирус Касперского осуществляет антивирусную проверку почтового трафика на уровне протокола передачи данных (POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих) независимо от используемой почтовой программы. Для популярных почтовых программ – Microsoft Outlook, Microsoft Outlook Express и The Bat! – предусмотрены плагины и лечение вирусов в почтовых базах.
- Проверку интернет-трафика. Kaspersky 7.0 обеспечивает антивирусную проверку интернет-трафика, поступающего по HTTP-протоколу, в режиме реального времени и независимо от используемого браузера. Это позволяет предотвратить заражение еще до сохранения файлов на жестком диске компьютера.
- Сканирование файловой системы. Проверке могут быть подвергнуты любые отдельные файлы, каталоги и диски. Кроме того, можно запустить проверку только критических областей операционной системы и объектов, загружаемых при старте Windows.

Основное отличие Антивируса Касперского в том что:

- Антивирус Касперского 7.0 – это классическая защита компьютера от вирусов, троянских и шпионских программ, а также от любого другого вредоносного ПО.
- Kaspersky Internet Security 7.0 – это программа для комплексной защиты ПК от вирусов и всех других типов вредоносных программ, а также от хакерских атак и спама.