**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ**

**И.Т. ТРУБИЛИНА»**

Прикладной информатики **факультет**

**Кафедра** Компьютерных технологий и систем

**КУРСОВАЯ РАБОТА**

Компьютерная вирусология

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность «Создание, поддержка и администрирование информационных систем»

Выполнила:

Шелудько Анастасия Александровна

Группа ИТ2202

Руководитель:

Ф.И.О.

*подпись*

**Дата защиты**



**Оценка**

Ф.И.О

*подпись*



**Краснодар 2022**

ОГЛАВЛЕНИЕ

[ВВЕДЕНИЕ 3](#_Toc117041789)

[Глава 1. ОБЩИЕ СВЕДЕНИЯ О КОМПЬЮТЕРНЫХ ВИРУСАХ 4](#_Toc117041790)

[1.1 Понятие компьютерных вирусов 4](#_Toc117041791)

[1.2 Классификация вирусов 5](#_Toc117041792)

[1.3 Вредоносное ПО и вирусы, их различия, пути происхождения 6](#_Toc117041793)

[Глава 2. АНАЛИТЕЧСКОЕ ИССЛЕДОВАНИЕ ВИРУСОВ 10](#_Toc117041799)

[2.1 Признаки и методы анализа появления вирусов. 10](#_Toc117041800)

[2.2 Методы обнаружения вредоносных программ. 14](#_Toc117041801)

[2.3 Антивирусы, их виды и сравнение лучших приложений. 16](#_Toc117041802)

[ЗАКЛЮЧЕНИЕ 20](#_Toc117041803)

[СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ 21](#_Toc117041804)

### ВВЕДЕНИЕ

Исследования в области компьютерной вирусологии до сих пор вызывают споры. Существует широко распространенное заблуждение, что исследования в области распространения компьютерных вирусов не интересны и не продуктивны: это потенциально опасно, поскольку данное суждение может привести к развитию более разрушительных методов вирусной атаки. Это широко распространенное мнение объясняет, почему существует совсем немного достойных исследований в университетах по всему миру, которые занимаются компьютерной вирусологией. В перспективе эти результаты демонстрируют, что, наоборот, глубокие исследования в области компьютерной вирусологии абсолютно необходимы, чтобы поддерживать эффективную защиту наших систем, а также попытаться предвидеть опасные компьютерные вирусы до того, как они внедрятся в наши устройства. Вирусы есть и, несомненно, останутся в компьютерном сообществе. Многие рассказы о схватках с компьютерными вирусами содержат изрядную долю приукрашивания, и многие компьютерные сбои, приписываемые вирусам, на самом деле происходят из-за «ошибки пилота». В этой статье рассматривается прошлое и текущее состояние компьютерных вирусов и «защитных вычислений», а также степень, ситуации, которая была омрачена шумихой, дезинформацией и непониманием. Хотя появление термина «компьютерный вирус» принадлежит Фреду Коэну в связи с его академическим исследованием платформы DEC VAX в 1983 году (Cobb, 1998), это явление не вызывало беспокойства у пользователей прикладных систем почти десять лет спустя. В 1987 году впервые возникли упоминания о данной проблеме в нескольких университетах, а вскоре после этого и в корпоративной среде. В современных условиях угроза компьютерных вирусов так или иначе затрагивает каждого пользователя компьютера. Однако степень воздействия не столь очевидна.

### Глава 1. ОБЩИЕ СВЕДЕНИЯ О КОМПЬЮТЕРНЫХ ВИРУСАХ

### 1.1 Понятие компьютерных вирусов

Компьютерный вирус — это вредоносный код, который воспроизводится путем копирования себя в другую программу, загрузочный сектор или документ компьютера и изменяет его работу. Данная программа схожа по принципу действия с биологическими вирусами: проникая в организм, они начинают активно размножаться внутри тела, тем самым заражая остальные клетки. Проводя аналогию с биологическим термином, также наблюдается, что своевременное лечение инфекции, дает большую вероятность устранения симптомов или вовсе искоренения вируса. Что касается компьютерной среды, все идентично. Вредоносные программы также умеет трансформироваться в едва заметные файлы, поэтому каждому пользователю следует знать о возможных структурах, состояниях, а также классификации вирусов.

### 1.2 Классификация вирусов

Согласно современным данным, существует 4 типа классификации вирусов.

Зависящие непосредственно от среды обитания

**Сетевые вирусы**, часто распространяемые на таких интернет-ресурсах, как: электронная почта, мессенджеры.

**Файловые вирусы**, в основном начинают заражение в исполняемых программах или файлах.

**Вирусы загрузочного сектора дискеты**, эти типы вирусов воздействуют на жесткий диск, либо делают запуск операционной системы невозможным.

**Макровирусы**: заражают приложение Microsoft Word или аналогичные ему, вызывают последовательность действий, которая выполняется автоматически, когда приложение запущено или что-то еще вызывает его.

**Комбинированные макровирусы**: тоже, что и обычные макровирусы, но имеют возможность к рассылке данных по электронной почте.

По выбору способа заражения окружающей среды

Различают 2 типа таких вирусов: **резидентные и нерезидентные**. Суть первого заключается в оставление той части вируса, которая непосредственно переключает внимание оперативной системы к зараженным программам и закрепляется за ними. Нерезидентный вирус не затрагивает память компьютера и его действие на систему имеет ограниченное по времени воздействие.

По разрушительным признакам

Существует также 2 разделения вирусов, относящихся к данной категории: **безвредные и неопасные**. Эти вредоносные программы занимают память на вашем компьютере. Их различие между собой заключается в том, что **неопасные вирусы** могут сопровождаться звуковыми или графическими эффектами, в отличие от безвредных.

По алгоритму внедрения

**Компаньон-вирусы** и **Вирусы «черви»** отличаются своим способом распространения. Они не затрагивают файлы на устройствах, а узнают сетевые адреса других компьютеров и изменяют их на свои.

### 1.3 Вредоносное ПО и вирусы, их различия, пути происхождения

**Вредоносное ПО** — это вредоносное программное обеспечение, которое действует против интересов пользователя. Вредоносное ПО может повлиять не только на зараженный компьютер или устройство, но потенциально на любое другое устройство, с которым может взаимодействовать.

Вредоносное ПО, вирусы и вредоносный код являются родственниками, но не одним и тем же, поэтому только один вид антивирусного программного обеспечения для защиты от вредоносных программ не может предотвратить все угрозы. Он может существовать компьютерах и мобильных устройствах, и в зависимости от того, какую операционную систему использует устройство (Windows, Android, iOS или Apple MacOS), вредоносное ПО может атаковать и представлять по-разному. После установки вредоносное ПО часто пытается украсть личные данные или заработать на пользователе. Чтобы лучше понять, что могут делать вредоносные программы и как снизить риски, нужно разбить распространенные типы вредоносных программ на категории.

**Троянский конь**

Троянский конь или «троян» распространяется с помощью социальной инженерии. Выдавая себя за что-то другое, троянец убеждает невольных пользователей установить его. Одна из распространенных стратегий заключается в том, чтобы злоумышленник убедил пользователя открыть файл или веб-ссылку, которая устанавливает вредоносное ПО. Например, такие трояны, как программы-пугалки, могут заставить пользователя думать, что конкретная программа поможет защитить его компьютер, хотя на самом деле программа делает обратное.

В других случаях пользователь может установить приложение, которое кажется полезным — например, стильную панель инструментов браузера или забавную клавиатуру с эмодзи, — но оно также содержит вредоносное ПО. Другой метод троянов заключается в записи автоматически устанавливаемого вредоносного ПО на USB-накопитель и передаче его ничего не подозревающему пользователю. Вредоносное ПО Remote Access Trojans (RAT) позволяет киберпреступникам удаленно управлять вашим устройством после проникновения.

## **Черви**

## Первые экспериментальные компьютерные черви, которые просто копировали себя, появились в 1970-х годах. Более опасные черви появились в 1980-х годах и стали первыми широко известными компьютерными вирусами, распространяющимися от ПК к ПК через дискеты и портя файлы, к которым у них был доступ. По мере распространения Интернета разработчики вредоносных программ и хакеры создавали червей, которые копировали себя в сетях, что делало их ранней угрозой для организаций и пользователей, подключенных к Интернету.

**Эксплойт**

Эксплойт — это уязвимость в программном обеспечении, которая может быть незаконно использована для того, чтобы заставить программное обеспечение делать что-то помимо того, для чего оно было предназначено. Часть вредоносного ПО может использовать эксплойт для проникновения в систему или перемещения из одной части системы в другую. Многие эксплойты основаны на известных уязвимостях (также называемых CVE), рассчитывая на то, что не все пользователи обновляют свои системы с помощью обновлений безопасности. Реже эксплойт нулевого дня использует критическую уязвимость, которая не была исправлена ​​специалистом по сопровождению программного обеспечения.

**Фишинг**

Фишинг — это форма социальной инженерии, при которой злоумышленник пытается обманом заставить кого-то передать конфиденциальную информацию или личные данные с помощью мошеннического запроса, такого как поддельное электронное письмо или мошенническое предложение. В качестве стратегии получения паролей и учетных данных для входа фишинговые атаки иногда предшествуют атаке вредоносных программ.

**Руткиты и Буткиты**

Руткит — это набор программных средств, предназначенных для получения полного контроля над системой и последующего заметания следов. Руткиты эффективно заменяют обычный административный контроль системы. Буткит — это расширенный вид руткита, который заражает систему на уровне ядра, поэтому он имеет еще больший контроль и его еще труднее обнаружить.

**Рекламное и шпионское ПО**

Рекламное ПО загромождает ваше устройство нежелательной рекламой, например всплывающими окнами в веб-браузере. Его близкий родственник-шпион собирает вашу информацию и передает ее куда-то еще. Шпионское ПО может варьироваться от трекеров, отслеживающих вашу интернет-активность, до сложных инструментов шпионажа. Шпионское ПО может включать в себя регистраторы нажатий клавиш или кейлоггеры, которые записывают все, что вводит пользователь. Шпионское и рекламное ПО не только нарушает вашу конфиденциальность, но и может замедлить работу вашей системы и засорить вашу сеть.

**Ботнеты**

Вредоносная программа - ботнет передает контроль над устройством внешней стороне, делая устройство частью большой сети зараженных устройств. Ботнеты обычно используются для проведения распределенных атак типа «отказ в обслуживании» (DDoS), рассылки спама или майнинга криптовалюты. Любое незащищенное устройство в сети может быть уязвимо для заражения. Ботнеты обычно имеют средства для расширения своей сети устройств и достаточно сложны, чтобы выполнять несколько вредоносных действий одновременно или последовательно. Например, при атаке вредоносного ПО Mirai в 2016 году использовались подключенные к Интернету камеры и домашние маршрутизаторы для создания массивной бот-сети DDoS.

**Программы-вымогатели**

Программа-вымогатель — это вредоносное ПО, требующее оплаты за что-либо. Многие распространенные виды программ-вымогателей шифруют файлы в системе пользователя и требуют выкуп в биткойнах в обмен на ключ дешифрования. Программы-вымогатели стали заметны в середине 2000-х годов. С тех пор атаки программ-вымогателей продолжают оставаться одной из самых серьезных и распространенных угроз компьютерной безопасности.

### Глава 2. АНАЛИТИЧЕСКОЕ ИССЛДЕОВАНИЕ ВИРУСОВ.

### **2.1 Признаки и методы анализа появления вирусов**.

Чтобы определить присутствует ли заражение вирусами, каждому пользователю следует знать основы компьютерной безопасности. Несмотря на обилие видов проявления вирусной атаки существуют основные признаки обнаружения вредоносных программ, которых стоит придерживаться.

* Замедленная работа компьютера.
  + Не всегда низкая скорость отклика пк говорит о угрозе, иногда это говорит о неисправности оборудования или его повреждения. В этом случае лучше всего обратиться к диспетчеру задач на вашем пк и оценить работу оперативной памяти, центрального процессора. Если нагрузка на центральный процессор приблизительно равна 100 %, то вероятность заражения устройства весьма велика. Невозможность загрузки операционной системы.
* Невозможность загрузки операционной системы.
  + Невозможность запуска, блокировка, сбои, неизвестные ошибки и всплывающие окна – все это свидетельствует о поражении вирусами или иным вредоносным ПО операционной системы. В основном данная проблема решается простым удалением вирусов или же чисткой реестра, но иногда приходится и полностью переустанавливать систему Windows.
* Исчезновение файлов и каталогов или искажение их содержимого.
  + Когда происходит неизвестное исчезновение файлов и каталогов, искажение информации, находящейся в них, то это означает, что скорее всего вирусом, который вредит вашему устройству, является так называемый «червь». Зачастую результатом работы этого вируса является шифровка ваших данных, а в последствии вымогание денег у жертвы за декодирование и нераспространение данных. Расшифровка в таком случае очень дорогой и сложный процесс, поэтому для избежания подобных случаев атаки следует дублировать данные.
* Исчезновение антивируса.
  + Частое проявление нахождения на устройстве вирусов, так как многие виды вирусов умеют не только блокировать программы по защите пк, а также и стирать с памяти устройства.
* Исчезновение доступа к сети.
  + Один из самых популярных признаков проявления вирусной активности. Появление всплывающих окон, медленная скорость интернета, сопровождают такого рода атаку.

Остальные проявления вирусных атак:

* много всплывающей рекламы
* не запускаются приложения
* увеличение файлов на диске
* появление незнакомых звуковых сигналов
* редактирование дат и времени файлов

Также стоит понимать, что все вышеперечисленные признаки могут быть вызваны не только вирусами, а также сбоями устройства или другими причинами. Из этого следует, что за правильным определением проблемы стоит обратиться к специалисту.

Анализ вредоносных программ — это шаг к обнаружению проблемы. Чтобы обнаружить вредоносное ПО, сначала мы должны проанализировать, как

оно выполняет свою функцию и какова цель его разработки. Методы анализа вредоносных программ делятся на три категории в зависимости от времени и техники.

**Статический анализ**

Когда программное обеспечение или часть кода анализируются без выполнения, то это называется статическим анализом. В этом методе программное обеспечение подвергается обратному проектированию с использованием различных инструментов и методов. Различные инструменты, которые можно использовать: отладчик, дизассемблер, декомпилятор и анализаторы исходного кода. Методы, которые используются при выполнении статического анализа включают проверку формата файла, извлечение строк, сканирование AV.

**Динамический анализ**

Рассмотрение функциональности программного обеспечения при выполнении называется динамическим анализом. Это можно сделать, проследив потоки управления, а также проанализировав инструкции, вызовы и параметры функций. Вредоносный код запускается в виртуальной среде для наблюдения за его поведением. Инструменты, которые используются для динамического анализа, — симулятор, эмуляторы RegShot, Process Explorer. Динамический анализ более эффективен, чем статический анализ, так как при использовании этого метода зараженное программное обеспечение запускается на виртуальной машине в целях мониторинга. Метод может легко обнаружить многие виды вредоносных программ, но данный тип анализа занимает больше времени, так как мы должны спроектировать среду для тестирования вредоносного ПО.

**Гибридный анализ**

Он сочетает в себе методы статического и динамического анализа, поэтому может использовать преимущества обоих подходов. Во-первых, программное обеспечение исследуется путем анализа кода вредоносного ПО, а затем запускается в виртуальной среде, чтобы наблюдать за его реальным поведением.

Если рассматривать два основных метода анализа вредоносного ПО, т.е статистический и динамический, то их основные различия в сравнении таковы:

**Таблица 1**

|  |  |
| --- | --- |
| **Статистический метод** | **Динамический метод** |
| Быстро и безопасно | Занимает достаточно большое количество времени и более уязвимо |
| Отлично проявляет себя в анализе много путёвого вредоносного ПО | Не справляется с анализом много путевого вредоносного ПО |
| Не может анализировать полиморфное вредоносное ПО | Не может анализировать полиморфное вредоносное ПО |
| Высокая точность результата исследования | Низкая точность результата исследования |

### 2.2 **Методы обнаружения вредоносных программ.**

Методы обнаружения вредоносных программ можно разделить на три категории: основанные на сигнатурах, основанные на эвристике и на основе спецификации. Эти методы идентифицируют и обнаруживают вредоносные программы и принимают контрмеры против них.

**Сигнатурный метод.**

Когда создается вредоносное ПО, в его код встраивается последовательность битов, известная как сигнатура. Данный метод можно использовать для определения того, к какому семейству принадлежит вредоносное ПО. Метод обнаружения на основе сигнатур используется большинством антивирусных программ. Антивирусная программа дизассемблирует код зараженного файла и осуществляет поиск шаблона, принадлежащего к семейству вредоносных программ. Сигнатуры вредоносных программ хранятся в базе данных, а в дальнейшем используются для сравнения в процессе следующих обнаружений. Сигнатурный метод может быть статическим, динамическим или гибридным.

**Эвристический метод**

Обнаружение на основе эвристики различает нормальное и ненормальное поведение системы, так что в конечном итоге известные и неизвестные вредоносные атаки могут быть идентифицированы и устранены. Эвристика состоит из двух этапов. На первом этапе поведение системы наблюдают в отсутствии атаки и ведут учет важной информации, которую можно проверить в случае атаки. Эта разница отслеживается на втором этапе для обнаружения вредоносного ПО определенного семейства.

**Метод на основе спецификации**

В методе обнаружения на основе спецификации проверяет нормальное и ненормальное поведение программы. Этот метод основан на эвристическом методе, но основное отличие состоит в том, что в методах обнаружения, основанных на эвристике, используются методы машинного обучения и искусственного интеллекта для обнаружения достоверных данных.

Располагая общей информацией об этих методах, можно выявить их преимущества и недостатки:

**Таблица 2**

|  |  |  |
| --- | --- | --- |
|  | **Преимущества** | **Недостатки** |
| **Сигнатурный** | * Прежде появлявшиеся вредоносные ПО легко могут быть замечены * Использует небольшое количество ресурсов в работе в отличие от остальных методов | Прежде не появлявшиеся вредоносные ПО не могут быть замечены |
| **Эвристический** | Прежде появлявшиеся и не появлявшиеся вредоносные ПО могут быть замечены | * Данные должны быть обновлены относительно новых и неизвестных * вредоносных программ * Нужно больше ресурсов с точки зрения времени и пространства * Низкая точность исследований |
| **Метод, основанный на спецификации** | * Прежде появлявшиеся и не появлявшиеся вредоносные ПО могут быть замечены * Высокая точность исследований | * Не эффективен в обнаружении новых вредоносных программ. * Разработка спецификации занимает много времени |

### 2.3 **Антивирусы, их виды и сравнение лучших приложений.**

Хотя просмотр веб-страниц или просмотр видео может показаться безобидным времяпровождением для обычного пользователя, однако существуют риски для вашего компьютера, скрывающиеся по всему Интернету. Различные типы вредоносных программ, уже известных нам как вирусы, могут использоваться для отслеживания того, что вы делаете в Интернете, и, возможно, для кражи вашей личной информации. Вот почему вам нужна антивирусная защита. Антивирусное программное обеспечение может сканировать информацию и файлы, отправляемые на ваш компьютер и с него, в режиме реального времени, когда вы просматриваете веб-страницы, отправляете электронные письма, смотрите потоковое видео или делаете что-либо еще в Интернете. Программное обеспечение предупредит вас, чтобы вы не нажимали на какие-либо веб-сайты или файлы, которые могут представлять угрозу вашей безопасности в Интернете. Кроме того, если вы случайно загрузите вредоносное ПО на свой компьютер, антивирусное программное обеспечение попытается поместить его в карантин и удалить, прежде чем оно причинит какой-либо вред вашему устройству. Чтобы грамотно подобрать антивирусную программу нужно понимать конкретное направление работы такого приложения. Рассмотрим основные методы поиска вирусов данными приложениями. Для обнаружения, защиты и удаления вредоносных программ разработаны такие виды антивирусных программ, как:

* Программы-доктора
* Программы-ревизоры
* Программы-детекторы
* Программы-фильтры
* Иммунизаторы
* Сканер

Рассмотрим каждый вид в отдельности:

**Программы-доктора**

Данные программы не только находят вирус на устройстве, но и устраняют из файла вредоносное тело, возвращая в файл в безопасное состояние

**Программы-ревизоры**

Являются одними из самых востребованных видов работы антивирусных программ. При поиске вируса обращается к загрузочному сектору жесткого диска, проверяет остальные файлы, смотрит наличие изменений реестра системы Windows и практически не использует обращение к оперативной памяти.

**Программы-детекторы**

Эти приложения ищут характерную сигнатуру для конкретного вируса файлах и оперативной памяти, при нахождении уведомляют об этом пользователя.

**Программы-фильтры**

Приложение представляет из себя резидентные программы, которые предназначены для обнаружения вредоносных программ.

**Иммунизаторы**

Это резидентные программы, которые предотвращают заражение файла. Корректное использование возможно только при наличии уже известных (для антивируса) вредоносных программ.

**Сканер**

Работа «сканера» основана на проверке файлов, системной памяти и секторов с помощью так называемой маски, последовательности кода для определенного вируса.

Чтобы определить какой антивирус нужен для конкретного пользователя, следует придерживаться данных правил:

На выбор антивируса большое значение оказывает мощность устройства. Так как защитная программа все-таки нагружает оперативную память, стоит обратить внимание на рекомендуемые разработчиком характеристики, позволяющие установить антивирусное приложение.

Если компьютер постоянно подключен к сети Интернет, то при выборе защитной программы следует обратить внимание на наличие функции сетевого экрана, который оберегает пользователя от попадания на небезопасные сайты, а также поможет избежать всплывающих окон.

Следует подумать над вопросом среды использования антивируса, так как не стоит использовать приложения для бизнеса в домашних условиях, ведь ваше устройство может не справится с столь серьезной нагрузкой.

Выбор стоит делать исходя из рейтингов реальных пользователей, актуальных и авторитетных источников информации, опираясь на верхние позиции.

Часто пользователь находится перед выбором – использовать бесплатные приложения или же оформлять ежемесячные подписки на определенном сервисе. Стоит понять, насколько важная информация находится на ее носителе. В любом случае всегда есть вероятность заражения вирусами, которые могут привести к потери данных. Рассчитывая на использование антивирусной программы в бизнес среде, стоит оставлять свой выбор за платной версией, так как это обеспечит быстрый отклик со стороны разработчика в случае заражения или утери данных.

### ЗАКЛЮЧЕНИЕ

Из всего исследования можно сделать вывод, что вирус — это программа, которая несет в себе небезопасную информацию, а также может выполнять нежелательные действия на компьютере. Некоторые компьютерные вирусы запрограммированы так, чтобы нанести вред вашему компьютеру, повреждая программы, удаляя файлы или переформатируя жесткий диск. Другие просто копируют себя или наводняют сеть трафиком, что делает невозможным выполнение какой-либо интернет-активности. Даже менее опасные компьютерные вирусы могут значительно снизить производительность вашей системы, истощая память компьютера и вызывая частые сбои компьютера. Несмотря на большое количество разновидностей вирусов, самовоспроизведение присуще всем разновидностям такого рода программ. В последнее время разрабатывается все больше вредоносных программ, поэтому самый простой способ для того, чтобы обезопасить свой компьютер — установить антивирусное приложение.

### СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

### Computer malware [электронный ресурс] <https://www.redhat.com/en/topics/security/what-is-malware>

### What is malware? [электронный ресурс] <https://www.redhat.com/en/topics/security/what-is-malware>

### Computer virus Coevolution [электронный ресурс] <https://dl.acm.org/doi/abs/10.1145/242857.242869>

### Virtual defence [электронный ресурс] <https://heinonline.org/HOL/LandingPage?handle=hein.journals/fora80&div=48&id=&page=>