**КУРСОВОЙ ПРОЕКТ**

**по дисциплине «Цифровой практикум»**

**«Вирусы»**

**Выполнил**

**студент группы 5130904/30002 Севостьянова А.В.**

**Руководитель**

**доцент, к.т.н Тутыгин В.С.**

Оглавление

[Введение 3](#_Toc150474517)

[1. Понятие «компьютерного вируса» 4](#_Toc150474518)

[2. История компьютерных вирусов 5](#_Toc150474519)

[Программа Creeper 5](#_Toc150474520)

[Вирус Rabbit 5](#_Toc150474521)

[Первый троянец 5](#_Toc150474522)

[Вирус загрузочного сектора Brain 5](#_Toc150474523)

[Вирус ILoveYou 6](#_Toc150474524)

[Червь Code 6](#_Toc150474525)

[Heartbleed 6](#_Toc150474526)

[3. Классификация компьютерных вирусов 7](#_Toc150474527)

[a. По среде обитания: 7](#_Toc150474528)

[b. По способу заражения: 7](#_Toc150474529)

[c. По деструктивным возможностям: 7](#_Toc150474530)

[d. По типу маскировки: 7](#_Toc150474531)

[*e.* По особенностям алгоритма работы: 7](#_Toc150474532)

[f. По вредоносной функциональности 8](#_Toc150474533)

[4. Способы заражения вирусом 9](#_Toc150474534)

[5. Признаки заражения компьютерным вирусом 10](#_Toc150474535)

[6. Основные средства борьбы с компьютерными вирусами 10](#_Toc150474536)

[Заключение 12](#_Toc150474537)

[Предметный указатель 13](#_Toc150474538)

[Список информационных ресурсов 14](#_Toc150474539)

# 

# Введение

Невозможно представить жизнь современного человека без компьютера. Его возможности используются в школе, на работе, при проведении досуга, в быту и других сферах жизни человека. Но, к сожалению, не все так хорошо как хотелось бы. Массовое использование персональных компьютеров привело к появлению программ-вирусов, препятствующих нормальному функционированию устройства, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

До середины XX века термин *«вирус»* (от лат. *virus* – яд, ядовитое начало) использовался лишь в медицине, обозначая инфекционного агента, вызывающего заболевание. С появлением, развитием и усложнением компьютерной техники, систем хранения, обработки и передачи информации, а также соответствующего программного обеспечения возник новый класс программ, известный теперь как *компьютерные вирусы*.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Персональный компьютер стал незаменимым помощником человека. Но столь глубокое проникновение в наши жизни такого необходимого устройства имеет и множество отрицательных сторон. Одна из них – компьютерные вирусы, о методах борьбы с которыми люди порой не имеют представления. **Актуальность темы моей работы** заключается в том, что сегодня каждому человеку необходимо владеть информацией о видах компьютерных вирусов и способах защиты ПК от них.

**Учебная цель:** изучение основных разновидностей компьютерных вирусов, методов борьбы с ними.

**Задачи курсовой работы:**

1. Изучить информацию по теме «компьютерные вирусы».
2. Выделить наиболее распространенные и известные компьютерные вирусы.
3. Составить классификацию компьютерных вирусов.
4. Выявить основные средства борьбы с вирусами, включая антивирусные программы.
5. Составить презентацию «Вирусы» для демонстрации результатов исследования.

**Объект исследования:** вредоносные программы – вирусы.

**Предмет исследования:** отрицательное воздействие компьютерных вирусов на ПК.

**Основные методы исследования:** изучение и анализ научной литературы, анализ полученной информации, метод обобщения.

**Практическая значимость работы:** составление презентации на тему «Вирусы»

2. **Понятие «компьютерного вируса»**

*Компьютерный вирус* – это специально написанная, небольшая по размерам программа (т.е. некоторая совокупность выполняемого кода), которая может приписывать себя к другим программам (заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере. Основная цель вируса – нарушение работы программ, порча файлов и каталогов, создания всевозможных помех в работе компьютера.

Программа, внутри которой находится вирус, называется *зараженной*. Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и заражает другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, засоряет оперативную память и т.д.). Ход работы вируса зависит от его типа.

Основными путями проникновения вирусов в компьютер являются *съемные внешние устройства*, а также *компьютерные сети*. Заражение жесткого диска вирусами может произойти при загрузке программы с внешнего устройства, содержащего вирус.

*Жизненный цикл* вируса обычно включает следующие периоды:

- Внедрение (попадание вируса на устройство).

- Инкубационный период (пассивное нахождение вируса на устройстве)

- Период саморазмножения (создание собственных копий).

- Проявление (проявление свойственных функций, например внос правок в пользовательскую информацию, искажение звука, повреждение файловой системы и т.д.).

Сама же структура компьютерного вируса достаточно проста. Вирус состоит из головы и хвоста (у некоторых видов компьютерных вирусов хвост отсутствует).

Под *головой* вируса понимается его часть, получающая доступ к программе первой. *Хвост* – это часть вируса, расположенная в тексте зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называются *несегментированными* и являются наиболее распространенной разновидностью компьютерных вирусов. Вирусы, содержащие голову и хвост, называются *сегментированными*.

# 

# 2. История компьютерных вирусов

Истрия компьютерных вирусов впервые обсуждалась в серии лекция математика Джона фон Неймана в конце 1940 годов. В 1960 году вышла его монография «Теория самовоспроизводящихся автоматов», которая рассматривала возможность существования «механического организма» (например, компьютерного кода), который мог бы повреждать машины, создавать собственные копии и заражать другие устройства по аналогии с биологическим вирусом.

## Программа Creeper

Первым вирусом считается программа Creeper, созданная в 1971 году сотрудником компании BBN Бобом Томасом. Creeper являлся тестовой программой, он проверял возможна ли в принципе самовоспроизводящаяся программа. Оказалось, что в некотором смысле возможна. Заразив новый жесткий диск, Creeper пытался удалить себя с предыдущего компьютера. Creeper не совершал никаких вредоносных действий – он только выводил простое сообщение: "I'M THE CREEPER. CATCH ME IF YOU CAN!" (Я CREEPER. ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ!).

## Вирус Rabbit

Вирус Rabbit (также известный как Wabbit) был создан в 1974 г. с вредоносной целью и мог самовоспроизводиться. Попав на компьютер, он делал большое количество копий себя, значительно ухудшал работоспособность системы и в итоге приводил к отказу компьютера. Имя («Кролик») было дано вирусу из-за того, что он очень быстро самовоспроизводился.

## Первый троянец

Первый троянец по названием ANIMAL (хотя есть споры относительно того, были ли это действительно троянец или просто вирус) был разработан программистом Джоном Уолкером в 1975 г. В то время были очень популярны компьютерные игры, в которых пользователь загадывал какое-нибудь животное, а программа должна была его угадать за 20 вопросов. Уолкер написал одну из таких игр, и она стала популярной. Чтобы поделиться ее со своими друзьями, Уолкер записывал и передавал ее на магнитной ленте. Чтобы упростить эту процедуру, Уолкер создал программу PERVADE, которая устанавливалась на компьютер вместе с игрой ANIMAL. Пока пользователь играл в игру, PREVADE проверял все доступные пользователю директории на компьютере, а затем копировал ANIMAL во все директории, где этой программы не было. Вредоносной цели здесь не было, но ANIMAL и PREVADE подпадают под определение троянца: по сути, внутри программы ANIMAL была запрятана другая программа, которая выполняла действия без согласия пользователя.

## Вирус загрузочного сектора Brain

Brain, первый вирус для IBM-совместимых компьютеров, появился в 1986 году – он заражал пятидюймовые дискеты. Как сообщает Securelist, вирус был написан двумя братьями – Баситом и Амджадом Фаруком Алви, которые держали компьютерный магазин в Пакистане. Братьям надоело, что покупатели нелегально копировали купленное у них ПО, и они создали этот вирус, которые заражал загрузочные сектора дискет. Brain заодно оказался и первым вирусом-невидимкой: при обнаружении попытки чтения зараженного сектора диска вирус незаметно подставлял его незараженный оригинал. Также он записывал на дискету фразу «(c) Brain», но при этом не портил никаких данных.

## Вирус ILoveYou

В начале 21 века появился надежный высокоскоростной интернет-доступ, и это изменило методы распространения вредоносных программ. Теперь они не были ограничены дискетами и корпоративными сетями и могли очень быстро распространяться через электронную почту, популярные веб-сайты и даже напрямую через интернет. Начало формироваться вредоносное ПО в современном виде. Ландшафт угроз оказался заселенным вирусами, червями и троянцами. Возник собирательный термин «вредоносное ПО». Одна из самых серьезных эпидемий новой эры была вызвана червем ILoveYou, который появился 4 мая 2000 г.

ILoveYou следовал модели ранее существовавших вирусов, распространявшихся по почте. При этом, в отличие от макровирусов, широко распространенных с 1995 года, ILoveYou распространялся не в виде зараженного документа Word, а в виде VBS-файла (такое расширение имеют скрипты, написанные в Visual Basic). Метод оказался простым и действенным – пользователи еще не привыкли остерегаться незапрошенных электронных писем. В качестве темы письма была строчка «I Love You», а в приложении к каждому письму был файл «LOVE-LETTER-FOR-YOU-TXT.vbs». По задумке создателя Онеля де Гузмана, червь стирал существующие файлы и поверх них записывал собственные копии, благодаря которым червь рассылался по всем адресам из списка контактов пользователя. Поскольку письма, как правило, приходили со знакомых адресов, получатели обычно открывали их – и заражали червем свой компьютер. Таким образом, ILoveYou на практике подтвердил эффективность методов социальной инженерии.

## Червь Code

Червь Code Red был так называемым бестелесным червем – он существовал только в памяти и не предпринимал попыток заразить файлы в системе. Используя брешь в системе безопасности Microsoft Internet Information Server, червь всего за несколько часов распространился по всему миру и вызвал хаос, внедряясь в протоколы обмена информацией между компьютерами. Зараженные компьютеры в итоге были использованы для проведения DDoS-атаки на веб-сайт Белого дома – Whitehouse.gov.

## Heartbleed

Угроза Heartbleed появилась в 2014 г. и сразу поставила под угрозу множество интернет-серверов. В отличие от вирусов и червей, Heartbleed – это уязвимость в OpenSSL – криптографической библиотеке универсального применения, широко использующейся по всему миру. OpenSSL периодически рассылает соединенным устройствам специальные сигналы, подтверждающие актуальность соединения. Пользователи могут отослать некоторый объем данных и в ответ запросить такое же количество данных – например, отослать один байт и получить в ответ тоже один байт. Максимальное количество данных, отправляемых за один раз – 64 килобайта. Как объясняет специалист по безопасности Брюс Шнайер, пользователь может объявить, что отсылает 64 килобайта, а по факту отправить только один байт – в этом случае сервер в ответ пришлет 64 килобайта данных, хранящихся в его оперативной памяти, в которых может оказаться все что угодно – от имен пользователей до паролей и криптостойких ключей.

**3. Классификация компьютерных вирусов**

Условно вирусы подразделяются на классы по следующим признакам:

1. По среде обитания:

*- Сетевые (в*ирусы, распространяющиеся по компьютерной сети).

*- Файловые (в*ирусы, внедряющиеся в выполняемый файл).

*- Загрузочные (в*ирусы, внедряющиеся в загрузочный сектор жесткого диска или дискеты).

*- Файлово-загрузочные* вирусы (вирусы, заражающие одновременно файлы и загрузочные сектора диска).

*- Макро-вирусы (в*ирусы~~,~~ заражающие текстовые документы редактора Microsoft Word).

*- «Flash» вирусы (*вирусы, поражающие микросхемы FLASH памяти (память для цифровых данных на базе микросхем, разновидность полупроводниковых запоминающих устройств; используются, например, во всех USB флешках).

1. По способу заражения:

*- Резидентные (*загружаемые в память ПК).

- *Нерезидентные (*не заражающие память ПК и остающиеся активными ограниченное время).

1. По деструктивным возможностям:

*- Условно-безвредные (*не влияющие на работу ПК).

*- Неопасные (*влияние ограничивается уменьшением свободной памяти на диске и графическими звуковыми и прочими эффектами).

*- Опасные (*приводят к серьезным сбоям в работе ПК).

*- Очень опасные (*приводят к потере программ, уничтожению данных, стиранию информации в системных областях памяти и даже преждевременному выходу из строя периферийных устройств).

1. По типу маскировки:

*- Невидимые вирусы*

Многие резидентные вирусы (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения DOS (операционной системы и прикладных программ) к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде.

*- Самомодифицирующиеся вирусы*

Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения – модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры этой кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус.

*- Вирусы, не использующие маскировк*

1. По особенностям алгоритма работы:

*- Черви*

Червями принято называть сетевые вирусы. Они проникают в память из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии. Черви проникают на устройство без каких-либо действий со стороны пользователя. Они ближе всех остальных вирусов подобрались к модели своих биологических прототипов и потому чрезвычайно разрушительны и опасны.

*- Бестелесные черви*

Вирусы, в процессе заражения и распространения не использующие ни временных, ни постоянных файлов. Они пробираются на компьютеры через бреши в системах безопасности и существуют исключительно в виде пакетов данных, передаваемых по коммуникационным каналам, или в виде программного кода в памяти зараженного компьютера.

*- Вирусы-спутники*

Вирусы поражают файлы путем создания файлов-двойников. При запуске программы сначала запускается файл с вирусом, а после выполнения своей работы вирус запустит незараженный файл. При таком способе заражения «инфицированная» программа не изменяется.

*- Паразитические вирусы*

Вирусы, которые модифицируют содержимое файлов или секторов на диске. К этой категории относятся все вирусы, не являющиеся вирусами-спутниками и вирусами червями.

*- Полиморфные вирусы*

Достаточно трудно обнаруживаемые вирусы, не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и доработками программы-расшифровщика.

*- Макровирусы*

Вирусы, использующие возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

*- Троянские программы (квазивирусы)*

Программы, которые не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

*- Студенческие вирусы*

Представляют собой самые простые и легко обнаруживаемые программы.

1. По вредоносной функциональности

*- Бэкдор (тайный вход)*

Дефект алгоритма, который намеренно встраивается разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

*- Кейлогеры (Keylogger – от англ. key – клавиша и logger – регистрирующее устройство)*

Программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя, например: нажатия клавиш на клавиатуре компьютера, на мыши и т. д.

*- Ботнеты*

Компьютерная сеть, состоящая из некоторого количества устройств с запущенными на них ботами (независимая программа). Чаще всего бот в составе сети скрытно устанавливается на устройство жертвы и позволяет злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера.

*- Руткиты*

Вирусы-гибриды, содержащие в себе различные вирусы. Получают доступ к персональному компьютеру, маскируют различные вирусы, собирают данные о компьютере и обо всех его процессах.

*- Вирусы-шпионы*

Программа, которая скрытым образом устанавливается на компьютер, с целью сбора информации о компьютере, копировании информации из памяти устройства, копировании данных пользователя, аудио/видеозаписи пользователя или пользовательской активности.

**4. Способы заражения вирусом**

Итак, как же происходит заражение компьютерными вирусами или вредоносными программами? Существует несколько стандартных способов. Это *зараженные файлы и ссылки на сайты, содержащие зараженные файлы, в электронной почте или сообщениях в социальных сетях, посещение такого сайта* *и использование зараженного USB-накопителя на вашем компьютере.* Уязвимости операционной системы и приложений позволяют злоумышленникам устанавливать вредоносное ПО на компьютеры. Поэтому для снижения риска заражения очень важно устанавливать обновления для операционной системы и приложений, как только они становятся доступными.

Киберпреступники часто используют методы социальной инженерии, чтобы обманом заставить вас делать что-то, что угрожает вашей безопасности. Фишинговые сообщения являются одним из наиболее распространенных методов. Вы получаете электронное сообщение, в котором вас убеждают загрузить зараженный файл или посетить вредоносный веб-сайт. Цель хакеров - написать сообщение так, чтобы вы нашли его убедительным. Это может быть, например, предупреждение о возможном вирусном заражении или уведомление из вашего банка или сообщение от старого друга.

Конфиденциальные данные, такие как пароли и персональные данные, являются главной целью киберпреступников. Помимо использования вредоносных программ для перехвата паролей в момент их ввода, злоумышленники также могут собирать пароли с веб-сайтов и других компьютеров, которые они взломали. Вот почему так важно использовать уникальный и сложный пароль для каждой учетной записи. Он должен состоять из 15 и более символов, включающих буквы, цифры и специальные символы. Таким образом, если киберпреступникам удастся взломать один аккаунт, они не получат доступ ко всем вашим учетным записям.

**5. Признаки заражения компьютерным вирусом**

Хотя большинство вредоносных программ не оставляет никаких явных следов, и ваш компьютер работает нормально, иногда все же можно заметить признаки возможного заражения.

* Медленная загрузка программ
* Перегрузка компьютера
* Частые системные ошибки
* Появление странных звуков, которые раньше не проявлялись
* Самопроизвольное открывание CD/DVD привода, или появление звуков, соответствующих чтению диска, хотя в приводе он отсутствует
* Длительный процесс включения или выключения компьютера
* Частое обращение к жесткому диску, что может свидетельствовать о наличии вирусов на самом диске.

**6. Основные средства борьбы с компьютерными вирусами**

Можно выделить три основные группы средств, которые помогут либо не допустить заражение компьютера вирусами, либо справиться с уже присутствующими вредоносными программами.

К этим группам относятся:

1. *Профилактические меры, использование которых позволит уменьшить вероятность заражения вирусами*

* Использование современных операционных систем (ОС), которые имеют серьезную встроенную систему защиты от вирусов;
* Установка антивирусных программ, которые могут анализировать состояние ОС и устранять некоторые ошибки в системе и других установленных программах;
* Использование антивирусных программных продуктов известных производителей с автоматическим обновлением антивирусных баз;
* Включение автоматического обновления ОС для автоматической загрузки новых исправлений и заплаток;
* Постоянную работу на компьютере исключительно с правами пользователя, а не администратора, то есть использование прав администратора лишь в исключительных случаях, когда это действительно необходимо;
* Использование персонального сетевого экрана («Firewall»), контролирующего выход пользователя с компьютера в Интернет и защищающий от информационных атак из внешних источников;
* Ограничение физического доступа к компьютеру посторонних лиц;
* Использование проверенных внешних носителей информации;
* Отключение автозапуска с внешних носителей, что не позволит запускаться вредоносным программам, которые могут оказаться на этих носителях каким-то неизвестным пользователю образом.

1. *Общие меры, которые полезны для защиты не только от вирусов, но и от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя.*

Общие меры делятся на две основные разновидности:

* копирования информации – создание копий файлов и системных областей дисков
* разграничения доступа – позволяет предотвращать несанкционированное использование информации пользователя и обеспечивает защиту от изменений в программах вирусами

1. *Специализированные антивирусные программы для защиты от вирусов и борьбы с ними.*

# 

# Заключение

Данная работа посвящена изучению компьютерных вирусов и средств борьбы с ними. В настоящее время актуальность данной темы подтверждается не только жизнью, но и статистическими данными, характеризующими уровень распространения компьютерных вирусов. Можно привести массу фактов, свидетельствующих о том, что угроза информационным ресурсам возрастает с каждым днем, подвергая панике ответственных лиц в банках, на предприятиях и в компаниях во всем мире. И угроза эта исходит от компьютерных вирусов, которые искажают или уничтожают ценную информацию, что может привести к серьезным последствиям.

Компьютерный вирус - 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 компьютера. Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - в отсутствии средств защиты у операционной системы.

В ходе работы была изучена и проанализирована информация о компьютерных вирусах, составлена их классификация, а также названы основные признаки заражения устройства вирусами и основные методы борьбы с данными вредоносными программами.

# 

# Предметный указатель

Heartbleed 6

Бестелесные черви 8

Ботнеты 9

Вирус ILoveYou 6

Вирус Rabbit 5

Вирус загрузочного сектора Brain 5

Вирусы-спутники 8

Вирусы-шпионы 9

Кейлогеры 9

Компьютерный вирус 4

Макровирусы 8

Паразитические вирусы 8

Первый троянец 5

Полиморфные вирусы 8

Программа Creeper 5

Руткиты 9

Студенческие вирусы 8

Троянские программы (квазивирусы) 8

Черви 8

Червь Code 6

# 

# Список информационных ресурсов

1. Защита компьютера на 100 %. Сбои, ошибки и вирусы: Петр Ташков — Москва, Питер, 2011 г.- 288 с.
2. Компьютерные вирусы и борьба с ними: А. В. Михайлов — Санкт-Петербург, Диалог-МИФИ, 2011 г.- 104 с.
3. Энциклопедия «Касперского» — Режим доступа: https://encyclopedia.kasp

4. Статья «Краткая история компьютерных вирусов, что нам сулит будущее» — режим доступа: <https://www.kaspersky.ru/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>

5. Энциклопедия «Касперского» — Режим доступа: <https://encyclopedia.kaspersky.ru/>