## Front matter

lang: ru-RU
title: Вредоносные программы. Вирусы и антивирусы.
subtitle: Основы информационной безопасности
author:

- Бабенко К. А.
  institute:
- Российский университет дружбы народов, Москва, Россия
  date: 16 февраля 2024

## i18n babel

babel-lang: russian
babel-otherlangs: english

## Fonts

mainfont: PT Serif
romanfont: PT Serif
sansfont: PT Sans
monofont: PT Mono
mainfontoptions: Ligatures=TeX
romanfontoptions: Ligatures=TeX
sansfontoptions: Ligatures=TeX,Scale=MatchLowercase
monofontoptions: Scale=MatchLowercase,Scale=0.9

## Formatting pdf

toc: false
toc-title: Содержание
slide_level: 2
aspectratio: 169
section-titles: true
theme: metropolis
header-includes:

- \metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}
- '\makeatletter'
- '\beamer@ignorenonframefalse'
- '\makeatother'

# Информация

## Докладчик

:::::::::::::: {.columns align=center}
::: {.column width="70%"}


- Бабенко Константин Алексеевич
- студент группы НКАбд-01-23
- Российский университет дружбы народов


:::
::: {.column width="30%"}

:::
::::::::::::::

## Введение

Введение
Компьютерные вирусы и вредоносные программы стали неотъемлемой частью современной цифровой среды.
Они представляют собой серьезную угрозу для безопасности данных, конфиденциальности пользователей
и стабильности работы информационных систем. В этом докладе мы рассмотрим различные виды вирусов,
их механизмы воздействия, а также методы защиты от них при помощи антивирусного программного
обеспечения.

## Вредоносные программы

Вредоносные программы – это программы, намеренно разработанные и внедряемые для нанесения ущерба
компьютерам и компьютерным системам. Если работа программы повлекла непреднамеренный ущерб, это
обычно называют программной ошибкой.

Часто спрашивают, чем отличается вирус от вредоносной программы. Разница в том, что вредоносная
программа – это общий термин для ряда сетевых угроз, включая вирусы, шпионские программы,
рекламные программы, программы-вымогатели и другие типы вредоносных программ. Компьютерный вирус –
это один из видов вредоносных программ.

Вредоносные программы могут попасть в сеть в результате фишинга, открытия вредоносных вложений,
опасных загрузок, социальной инженерии и с переносных накопителей.

## Виды вредоносных программ:

1. Вирусы — это программы, способные прикрепляться к другим программам или файлам и
самовоспроизводиться. Они активируются при запуске зараженного файла и могут повредить систему,
удалить данные или изменить поведение программ.

2. Черви — это самостоятельные программы, которые распространяются по сетям, используя уязвимости
в системах. Они могут быстро размножаться и перегружать сеть трафиком.

3. Трояны маскируются под легитимные программы, но выполняют скрытые вредоносные функции. Они
могут красть данные, предоставлять злоумышленникам удаленный доступ к системе или устанавливать
другое вредоносное ПО.

4. Шпионские программы собирают информацию о пользователе и передают её третьим лицам. Это может
включать историю браузера, личные данные, пароли и другую конфиденциальную информацию.

5. Adware — это программы, которые показывают нежелательные рекламные объявления. Хотя некоторые
из них относительно безвредны, другие могут собирать личную информацию или перенаправлять
пользователя на мошеннические сайты.

6. Руткиты позволяют злоумышленникам получить полный контроль над системой, скрывая своё присутствие.
Они могут изменять настройки безопасности, отключать антивирусы и предоставлять удалённый доступ.

7. Криптовымогатели шифруют важные файлы пользователя и требуют выкуп за их расшифровку. Эти
программы особенно опасны, поскольку восстановление данных может оказаться невозможным даже после
уплаты выкупа.

8. Боты — это программы, которые превращают заражённые компьютеры в часть сети (ботнета). Ботнеты
используются для проведения DDoS-атак, рассылки спама, майнинга криптовалют и других нелегальных
действий.

9. Эксплойты — это программы или скрипты, использующие уязвимости в системах для получения
несанкционированного доступа или выполнения определённых действий. Они могут использоваться для
установки другого вредоносного ПО или получения контроля над системой.

10. Скрипты и сценарии могут выполнять вредоносные действия, такие как удаление файлов, изменение
настроек системы или отправка данных злоумышленникам. Они часто написаны

на языках программирования,
таких как JavaScript, VBScript или PowerShell.

11. Логическая бомба — это программа, которая срабатывает при выполнении определённых условий,
например, конкретной даты или события. Она может уничтожить данные, нарушить работу системы или
выполнить другие разрушительные действия.

12. Дроппер — это программа, предназначенная для загрузки и установки другого вредоносного ПО на
заражённую систему. Он может быть использован для обхода антивирусной защиты.

13. Пакеры сжимают и упаковывают вредоносные программы, чтобы затруднить их обнаружение антивирусными
средствами. Криптеры дополнительно шифруют содержимое, делая его ещё менее заметным.

14. Фишинг — это вид социальной инженерии, когда злоумышленники пытаются обманом заставить
пользователя раскрыть конфиденциальную информацию (пароли, номера карт и т.п.). Это может происходить
через поддельные сайты, электронные письма или сообщения.

## Компьютерный вирус и его особенности

Компьютерный вирус является одним из видов вредоносного программного обеспечения, однако он
обладает уникальными характеристиками, отличающими его от других типов вредоносных программ. Давайте
разберем, что такое компьютерный вирус и чем он отличается от других видов вредоносного ПО.

Компьютерный вирус — это программа, способная самовоспроизводиться и внедрять копии своего кода в другие
программы или файлы. Чтобы начать свою деятельность, вирусу требуется выполнение зараженной программы
или файла.

То-есть компьютерный вирус - это вредоносная программа, обладающая следующими свойствами:

- Саморазмножение: Вирусы способны создавать копии самого себя и внедрять эти копии в другие программы
  или файлы.
- Необходимость запуска: В отличие от некоторых других типов вредоносного ПО, вирус не начинает
  действовать сразу же после попадания на устройство. Ему нужно, чтобы пользователь запустил зараженную
  программу или файл.
- Изменение поведения системы: Вирусы могут изменять поведение системы, повреждать файлы, удалять данные

или нарушать нормальную работу устройства.
- Распространение: Вирусы могут распространяться через обмен файлами, электронную почту, съемные
носители и другие способы передачи данных.

Компьютерный вирус отличается от других видов вредоносного ПО своей способностью к самокопированию и
необходимости запуска зараженной программы пользователем. Другие типы вредоносного ПО, такие как черви,
трояны, шпионское ПО, криптовымогатели и бэкдоры, имеют свои уникальные характеристики и методы действия,
направленные на достижение разных целей, будь то сбор данных, получение удаленного доступа или
вымогательство денег.

## Типы вирусов

По механизму заражения:

- Резидентные. Достаточно установить вирус-резидент, чтобы он остался в памяти и продолжил искать новые
цели непрерывно, пока работает среда, в которой он действует.
- Нерезидентные. Вирусы выполняют однократный поиск целей, а затем передают управление заражённому объекту.

По степени опасности:

- Безопасные. Не наносят какого-либо ущерба компьютеру, за исключением расходования свободного места на
диске во время своего распространения.
- Безвредные. Не мешают работе компьютера, но занимают оперативную память и место на диске, их действия
проявляются в виде графических или звуковых эффектов.
- Опасные. Способны вызвать различные сбои в работе компьютера — например, перезагрузку, зависание и т.д.
- Очень опасные. От воздействия таких вирусов ПО, установленное на ПК, перестаёт нормально работать,
уничтожаются важные файлы, а в системных областях диска стирается информация, что приводит к повреждению
операционной системы.

По среде обитания:

- Загрузочные. Они сохраняются в первом секторе жёсткого диска, где вирусы активируются при загрузке ПК.
- Файловые. Эти вирусы операционной системы внедряются в исполняемые файлы операционной системы, создают
свои копии в папках каталогов и файлы-двойники.
- Макровирусы. Данные программы написаны на макроязыках, с помощью которых во многих текстовых,
графических и табличных редакторах, системах проектирования создаются функции-макросы, автоматизирующие
выполнение некоторых операций.

- Сетевые. Внедряются в компьютер вместе с заражёнными файлами через локальные сети или интернет.

По методу заражения файлов:

- Перезаписывающие. Такие программы полностью меняют код заражаемого файла на свой, в результате чего
  содержимое файла уничтожается.
- Паразитические. Они частично перезаписывают файлы при заражении, внедряя в них свой код, но оставляют
  их работоспособными.
- Компаньоны. Особенностью таких вирусов является то, что они не перезаписывают заражаемые файлы. Вместо
  этого они создают их двойники, которые и начинают работать при активации заражённого файла.
- Ссылочные. Данный тип также не перезаписывает заражаемые файлы. Однако когда ОС запускает такой файл,
  она выполняет код вируса за счёт изменения им соответствующих полей файловой системы.
- Файловые черви. Такие вирусы в системе копируют себя в файловые каталоги. Эти копии не активируются при
  выполнении какого-либо файла — они находятся в «спящем режиме» до того момента, когда пользователь сам
  активирует их.

## Антивирусы

Антивирусы — это специальные программы, предназначенные для обнаружения, предотвращения и удаления
вредоносных программ, таких как вирусы, черви, трояны, шпионское ПО и другие виды вредоносного программного
обеспечения (malware). Они играют ключевую роль в обеспечении безопасности компьютеров и мобильных устройств,
защищая их от потенциальных угроз.

Антивирусы используют несколько технологий для обнаружения и нейтрализации вредоносного ПО:

- Сигнатурный анализ: Сравнивает коды подозрительных файлов с базой данных известных вирусов. Если совпадение
  найдено, файл помечается как вредоносный и обрабатывается соответствующим образом.
- Эвристический анализ: Анализирует поведение программ и ищет аномалии, которые могут указывать на наличие
  вируса. Эта технология полезна для обнаружения новых или неизвестных угроз.
- Поведенческий анализ: Отслеживает действия программ в реальном времени и блокирует подозрительную активность,
  например, попытки изменения системных файлов или отправки данных на удаленные серверы.
- Облачные технологии: Использование облачных баз данных для быстрого обновления сигнатур и анализа новых
  угроз. Это позволяет антивирусам оперативно реагировать на новейшие угрозы.

- Проактивная защита: Предотвращает заражение до того, как оно произойдет, путем блокировки потенциально
  опасных действий.
- Мониторинг сети: Контроль входящего и исходящего трафика для выявления попыток проникновения вирусов.
- Файрволлы: Фильтрация сетевых пакетов и блокировка подозрительного трафика.
- Защита от фишинга: Распознавание поддельных сайтов и блокировка доступа к ним.
- Резервное копирование: Создание копий важных данных для восстановления после атаки.

## Заключение

Вредоносные программы продолжают развиваться и совершенствоваться, поэтому важно постоянно обновлять знания о
современных угрозах и использовать комплексные меры защиты. Регулярный мониторинг системы, своевременное
обновление ПО и соблюдение правил информационной безопасности помогут минимизировать риски и обеспечить
надежную защиту ваших данных.

:::