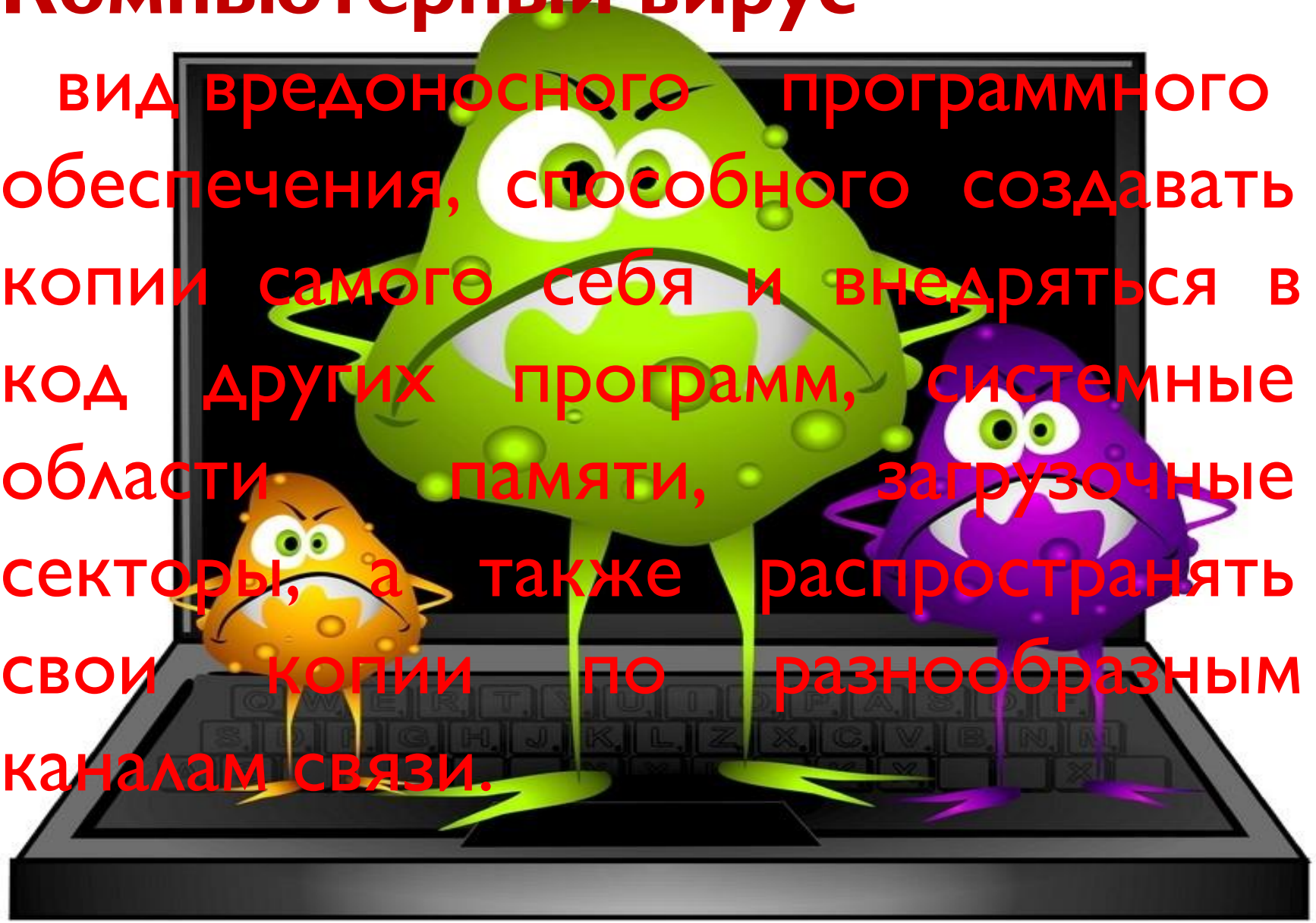
Компьютерные вирусы

Выполнила Леонова
Юлия Сергеевна

Компьютерный вирус—

вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.



Классификация компьютерных вирусов

- по поражаемым объекта
- по механизму заражения
- по поражаемым операционным системам и платформам
- по технологиям, используемым вирусом
- по языку, на котором написан вирус
- по дополнительной вредоносной функциональности

По поражаемым объектам:

- файловые вирусы
- загрузочные вирусы
- сценарные вирусы
- Макровирусы
- вирусы, поражающие исходный код

По механизму заражения:

- паразитирующие (добавляют себя в исполняемый файл)
- перезаписывающие (невосстановимо портят заражённый файл)
- «спутники» (идут отдельным файлом)

По пораженным операционным системам и платформам

- Вирусы поражающие DOS
- Вирусы поражающие Microsoft Windows
- Вирусы поражающие Unix
- Вирусы поражающие Linux

По технологиям, используемых вырусом:

- полиморфные вирусы(**Полиморфизм компьютерного вируса** (греч. πολυ- — много + греч.μορφή — форма, внешний вид) — специальная техника, используемая авторами вредоносного программного обеспечения для снижения уровня обнаружения вредоносной программы классическими антивирусными продуктами.)
- стелс-вирусы(**Стелс-вирус** (англ.*stealth virus* — вирус-невидимка) — вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)
- руткиты (**Руткит** (англ. *rootkit*, то есть «набор root'a») — набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), для обеспечения: маскировки объектов (процессов, файлов, директорий, драйверов);контроля (событий, происходящих в системе);сбора данных (параметров системы))

По языку на котором написан вирус:

- Ассемблер
- высокоуровневый язык программирования
- сценарный язык
- и др.

По дополнительной вредоносной функциональности:

- Бэкдоры (дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить тайный доступ к данным или удалённому управлению компьютером)
- Кейлоггеры (программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.)
- Шпионы (программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего. Также могут производить другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя.)
- Ботнеты (компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании
- и др.

СПАСИБО ЗА