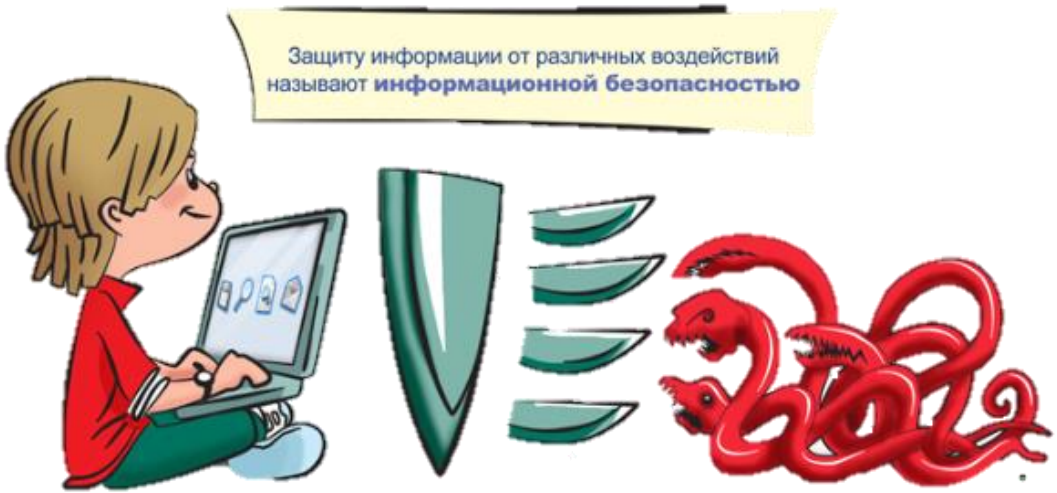
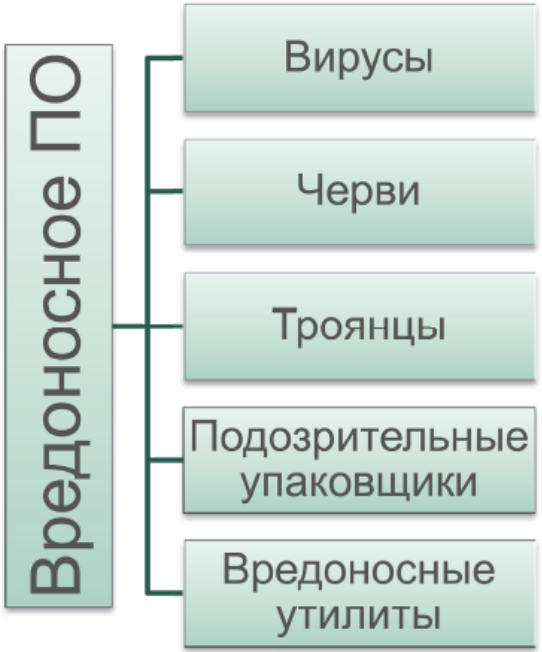
КЛАССИФИКАЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ

ВРЕДОНОСНЫЕ ПРОГРАММЫ

создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей



ВИДЫ ВРЕДОНОСНЫХ ПРОГРАММ (ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ)



ВИРУСЫ

Определение вируса по ГОСТ Р 51188-98 звучит так.

Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и **внедрять их в файлы**, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

в узком понимании,

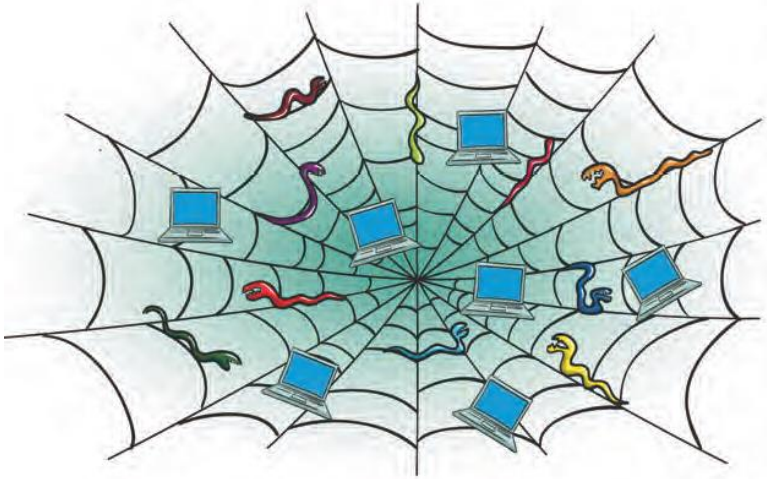
Вирус – это вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по локальным ресурсам компьютера.

ВИРУСЫ. КЛАССИФИКАЦИЯ

ЧЕРВИ

Программы, распространяющие свои копии через сеть с целью

- проникновения на удаленные компьютеры
- запуска на них своих копий
- возможного выполнения деструктивных действий
- дальнейшего распространения по сети



Сетевые черви — это вредоносные программы, которые тайком от пользователя быстро распространяются по компьютерной сети

ЧЕРВИ. КЛАССИФИКАЦИЯ

Email-Worm
(почтовые черви)

IRC-Worm
(черви в IRC-каналах)

IM-Worm
(черви, использующие интернет-пейджеры)

P2P-Worm
(черви для сетей обмена файлами)

Net-Worm
(прочие сетевые черви)

ТРОЯНСКИЕ ПРОГРАММЫ

Программы, действующие без ведома пользователя

- сбор информации и ее разрушение
- злонамеренное изменение данных и/или передача их злоумышленнику
- нарушение работоспособности системы
- использование ресурсов компьютера в злоумышленных целях

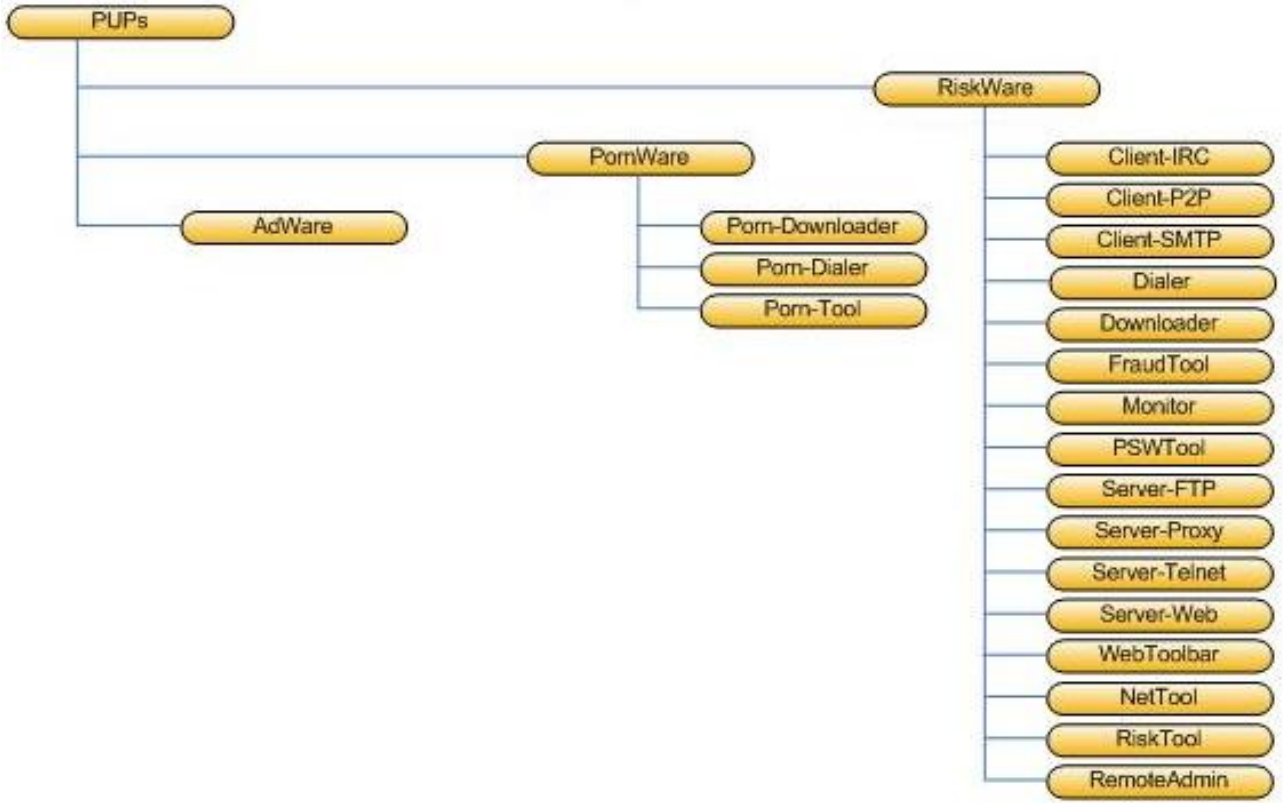
ТРОЯНСКИЕ ПРОГРАММЫ. КЛАССИФИКАЦИЯ

Backdoor	(удаленное администрирование)
Trojan-PSW	(воровство паролей)
Trojan-Clicker	(интернет-кликеры)
Trojan-Downloader	(доставка вредоносных программ)
Trojan-Dropper	(инсталляторы вредоносных программ)
Trojan-Proxy	(троянские прокси-серверы)
Trojan-Spy	(шпионские программы)
Trojan	(прочие троянские программы)
Rootkit	(сокрытие присутствия в ОС)
ArcBomb	(«бомбы» в архивах)
Trojan-Notifier	(оповещение об успешной атаке)

УСЛОВНО ОПАСНЫЕ ПРОГРАММЫ (PUPS)

- Разрабатываются и распространяются легальными компаниями
- Могут использоваться в повседневной работе
  - Например, утилиты удаленного администрирования и т.п.
- Обладают набором функций, которые могут причинить вред пользователю только при выполнении ряда условий
- Могут быть опасны в руках злоумышленника

УСЛОВНО ОПАСНЫЕ ПРОГРАММЫ



ХАКЕРСКИЕ УТИЛИТЫ И ПРОЧИЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ

- Сетевые атаки
- Взломщики удаленных компьютеров
- «Замусоривание» сети
- Конструкторы вирусов и троянских программ
- Злые шутки, введение пользователя в заблуждение
- Фатальные сетевые атаки
- Сокрытие от антивирусных программ
- Полиморфные генераторы
- Средства написания, изучения вирусов

СПАМ

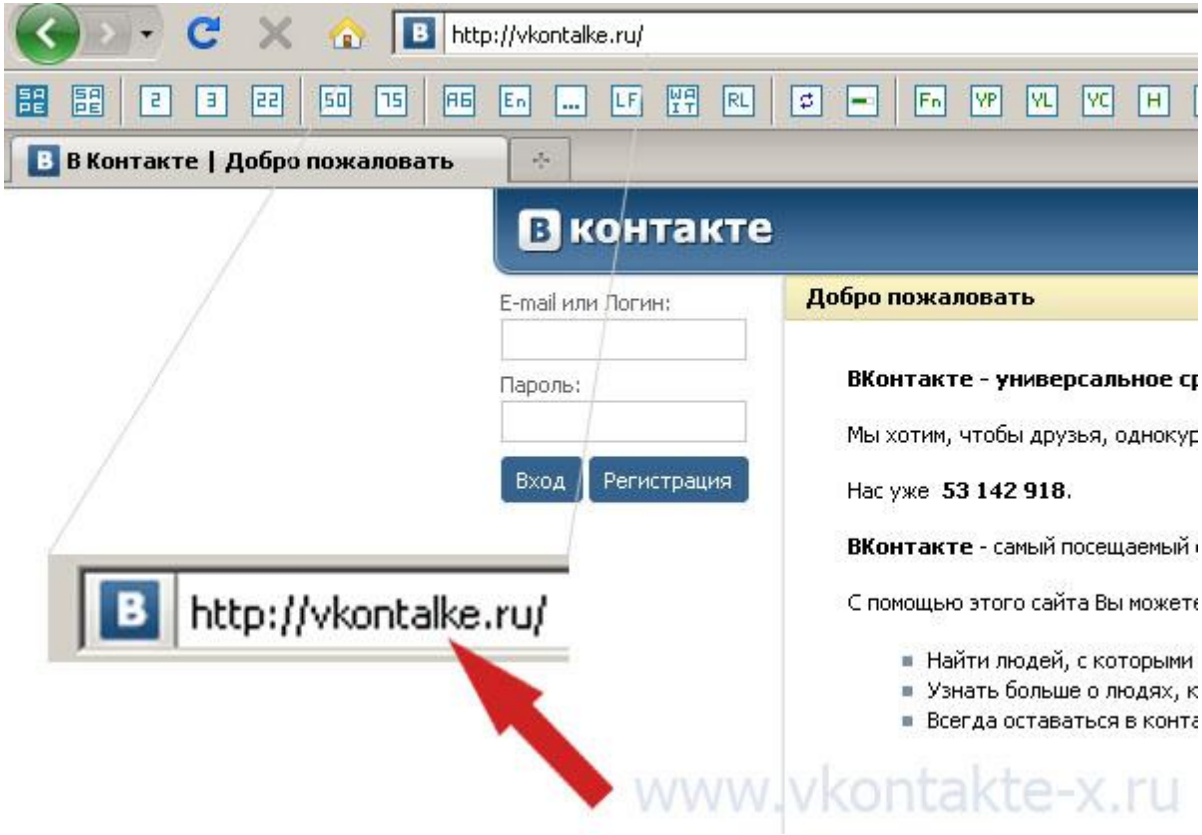

Спам (англ. *spam*) — сообщения, массово рассылаемые людям, не дававшим согласие на их получение. В первую очередь, термин «спам» относится к электронным письмам с различной рекламой

ФИШИНГ

- Фишинг — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

- Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных данных от электронной почты — эти данные могут пригодиться тем, кто рассылает вирусы или создает зомби-сети.

ФИШИНГ


http://vkontalke.ru/
В Контакте | Добро пожаловать
ВКонтакте
E-mail или Логин:
Пароль:
Вход
Регистрация
Добро пожаловать
ВКонтакте - универсальное ср
Мы хотим, чтобы друзья, однокур
Нас уже 53 142 918.
ВКонтакте - самый посещаемый
С помощью этого сайта Вы можете
Найти людей, с которыми
Узнать больше о людях, к
Всегда оставаться в конта
http://vkontalke.ru/
www.vkontakte-x.ru

ЧТО ДЕЛАТЬ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ?

Проверяйте на вредоносные программы все съёмные носители информации: дискеты, CD, DVD и флеш-диски, которые ранее использовались на другом компьютере.

Используйте только программы и данные, полученные из источников, которые вы знаете и которым доверяете. Чаще всего вирусами бывают заражены пиратские копии программ, особенно различных компьютерных игр.

Старайтесь не позволять другим людям работать с вашим личным компьютером.

Рекомендуется время от времени менять свои пароли.

Никогда не открывайте файлы, прикреплённые к электронным письмам, пришедшим от неизвестных вам отправителей. Не заходите на сайты, рекламируемые через «спам-рассылки» (сегодня большинство вирусов распространяются именно таким способом).

А ТАКЖЕ…


Соблюдайте
правила компьютерной гигиены!
Правильно и своевременно выполняя эти правила, можно предотвратить заражение компьютера или уменьшить ущерб, если заражение все-таки произошло

СПАСИБО!

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com