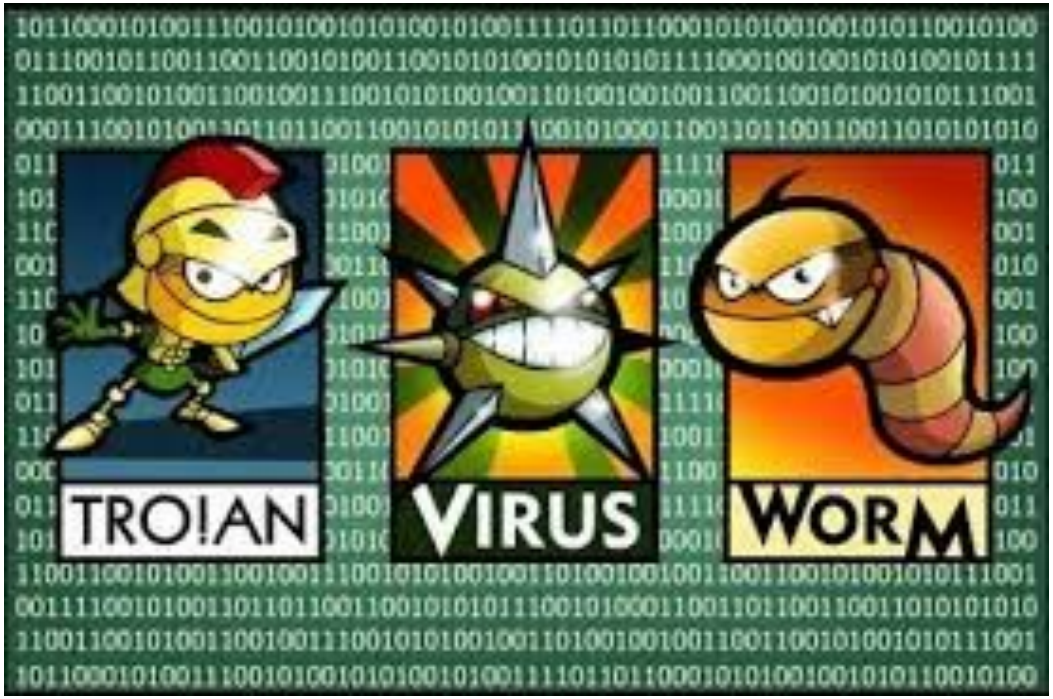
Вредоносное программное обеспечение и защита информации

Вредоносная программа

- Вредоносная программа - любое программное обеспечение, предназначенное для получения несанкционированного доступа к ресурсам компьютера, с целью несанкционированного использования ресурсов или нанесения ущерба владельцу информации (владельцу компьютера) путём копирования, искажения, удаления или подмены информации.
- Это программы, которые создают программисты специально для нанесения ущерба пользователям ПК. Их создание и распространение является **преступлением**

К вредоносному программному обеспечению относятся:

- компьютерные вирусы;
- сетевые черви;
- троянские программы;
- руткиты;
- бэкдор.



Компьютерный вирус

- **Вирус** - это программа, которая обладает способностью без предупреждения пользователя создавать свои копии и внедрять их в различные объекты и ресурсы компьютера и компьютерных сетей, нанося вред компьютеру.
- Вирусы можно подцепить разными способами: от нажатия вредоносной ссылки или файла в неизвестном письме до заражения на вредоносном сайте.
- Вирус может выполнять множество разных задач, направленных в первую очередь на принесение вреда операционной системе.
- В настоящее время вирусы довольно редки, так как создатели вредоносного ПО стараются держать свои программы и их распространение под контролем. В ...ктивном случае вирус довольно быстро попадает в руки ...тивирусных компаний.

Сетевые черви

- **Сетевой червь** — разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.
- Черви созданы на основе саморазмножающихся программ. Однако черви не могут заражать существующие файлы. Вместо этого червь поселяется в компьютер отдельным файлом и ищет уязвимости в Сети или системе для дальнейшего распространения себя.
- **Сетевые черви** распространяют свои копии по компьютерным сетям с целью:

✔ проникновения на удаленные компьютеры;

✔ запуска своей копии на удаленном компьютере;

✔ дальнейшего распространения на другие компьютеры в сети.

Троянские программы

Троянские программы проникают в компьютер под видом легального программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.

Троянские программы осуществляют различные несанкционированные пользователем действия:

- сбор информации и ее передачу злоумышленнику,
- ее разрушение или злонамеренную модификацию,
- нарушение работоспособности компьютера,
- использование ресурсов компьютера в неблаговидных целях.

Трояны

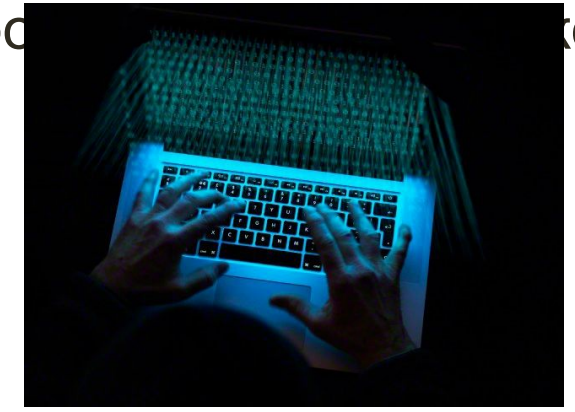
- По своему действию являются противоположностью вирусам и червям.
- Их предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности они делают то, что нужно злоумышленникам.
- Троянцы получили свое название от одноименного печально известного мифологического коня, так как под видом какой-либо полезной программы или утилиты в систему проникает деструктивный элемент.
- Трояны не самовоспроизводятся и не распространяются сами по себе. Однако с увеличением вала информации и файлов в Интернете трояна стало довольно легко подцепить.
- Нынешние трояны эволюционировали до таких сложных форм, как, например, бэкдор (троян, пытающийся взять на себя администрирование компьютера) и троян-загрузчик (устанавливает на компьютер жертвы вредоносный код).

Руткит

- Руткит представляет собой особую часть вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения.
- Это возможно благодаря тесной интеграции руткита с операционной системой.
- Некоторые руткиты могут начать свою работу прежде, чем загрузится операционная система. Таких называют буткитами.
- Однако, как бы ни развивался этот тип вредоносов, сложные современные антивирусные программы в состоянии обнаружить и обезвредить практически все существующие разновидности руткитов.

Бэкдор (средство удаленного администрирования)

- Бэкдор, или RAT (remote administration tool), — это приложение, которое позволяет честному системному администратору или злобному злоумышленнику управлять вашим компьютером на расстоянии.
- В зависимости от функциональных особенностей конкрентного бэкдора, хакер может установить и запустить на компьютере жертвы любое программное обеспечение, сохранять все нажатия клавиш, загружать и сохранять любые файлы, включать микрофон или камеру. Словом, брать на себя контроль за компьютеро жертвы.



Хакерские утилиты

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб компьютеру.

Основные признаки появления вирусов:

- Прекращение работы или неправильная работа ранее успешно функционировавших программ;
- Медленная работа компьютера;
- Невозможность загрузки операционной системы;
- Исчезновение файлов и каталогов или искажение их содержимого;
- Изменение даты и времени модификации файлов;
- Изменение размеров файлов;
- Неожиданное значительное увеличение количества файлов на диске;
- Существенное уменьшение размера свободной оперативной памяти;
- Вывод на экран непредусмотренных сообщений, изображений или звуковых сигналов;
- Частые зависания и сбои в работе компьютера.

Антивирусная программа

Антивирусная программа – это программа, предназначенная для обнаружения и удаления компьютерных вирусов, а также для эффективной защиты от них.

Антивирусные программы используют два различных метода для выполнения своих задач:

- 1) сканирование (просмотр) файлов для поиска уже известных вирусов, для которых в вирусной базе (входящей в комплект антивирусной программы специальной БД) есть информация о характерных фрагментах вирусного программного кода (сигнатурах вирусов);
- 2) обнаружение подозрительного поведения любой программы, которое похоже на поведение зараженной программы («эвристическое сканирование»).

Примеры антивирусных программ

Так как новые вирусы создаются непрерывно, то антивирусные программы требуется **регулярно обновлять**.

Примеры антивирусных программ: Norton AntiVirus, DoctorWeb, Symantec Antivirus, Антивирус Касперского, NOD32, av

Для защиты информации необходимо:

- периодически проверять все данные на компьютере на наличие вирусов;
- проверять информацию с принесенных носителей (дискеты, флэш);
- проверять информацию, полученную по сети;
- следить за своевременным обновлением антивирусных программ;
- иметь резервные копии системного диска и важной информации.

Помните!

За создание, использование и распространение вредоносных программ предусмотрена различная ответственность, в том числе и уголовная, в законодательстве многих стран мира.