**1. Вредоносные программы и антивредоносное программное обеспечение**

Классификация по вредоносной нагрузке:

1. Создание помех в работе оборудования;

2. Установка других вредоносных программ;

3. Использование для получения персональных данных и мошенничества.

По методу размножения:

1. Эксплойт - представляет собой набор данных, вызывающий ошибку при обращении к нему.

2. Логическая бомба - вредоносное действие совершается при выполнении некоторого условия;

3. Троянская программа - не имеет собственного механизма размножения.

4. Компьютерный вирус - размножается в пределах компьютера и через сменные носители.

5. Сетевой червь - способен самостоятельно размножаться по сети.

По среде обитания:

1. Файловые - внедрение в исполняемые файлы путем их дублирования (компаньон-вирусы) или использования особенностей организации файловой системы (link-вирусы).

2. Загрузочные - запись в загрузочный сектор диска (boot-сектор) или в сектор системного загрузчика жесткого диска (master boot record).

3. Макровирусы - использование возможности программ обработки информации для переноса тела вируса (Word, Excel и т.д.).

4. Сетевые - используют возможности протоколов компьютерных сетей.

Жизненный цикл вирусов.

1. Стадия хранения:

‑ хранение на носителе внедренным в объект;

‑ наиболее уязвим на данной стадии.

Способы защиты от обнаружения:

‑ шифрование части тела вируса;

‑ модификация кода загрузчика.

Модификация кода загрузчика. Цель — обеспечить текстуальные различия с оригиналом при неизменных результатах работы:

‑ изменение порядка независимых инструкций;

‑ замена части инструкций на эквивалентные по результату работы;

‑ введение зашумляющих инструкций.

Полиморфные вирусы — не имеют ни одного постоянного участка кода.

Стелс вирусы — обеспечивают собственное скрытие в системе за счет перехвата и контроля прерываний.

Резидентные вирусы — в оперативной памяти ПК оставляют свою резидентную часть, которая перехватывает прерывания ОС к объектам и заражает их.

2. Стадия исполнения:

‑ выполнение деструктивных действий;

‑ загрузка вируса;

‑ поиск жертвы;

‑ заражение жертвы;

‑ выполнение деструктивных функций;

‑ передача управления программе-носителю.

Способы распространения:

1. Электронная почта - маскирование “зараженных” исполняемых файлов под текстовые документы. Использование HTML ссылок на активные компоненты ActiveX, Java и т.д.

2. “Троянские” web-сайты - используются уязвимостей браузера для запуска на целевом ПК активных компонентов.

3. Локальная сеть - посредством внедрения тела вируса, в файлы, размещенные на сервере (login.com и т.д.).

Типовые признаки деятельности вируса:

‑ появление сообщений об ошибках;

‑ искажение наборов данных;

‑ истощение ресурсов ПК;

‑ невозможность загрузки ОС.

Общие способы защиты

1. Ограничение физического доступа.

2. Работа с правами пользователя.

3. Обновление ПО.

4. Отключение функции автозапуска в ОС.

5. Контроль за сменными носителями.

Методы обнаружения вирусов

1. Сравнение с эталоном - поиск вируса по его “маске”. Обнаружение известных вирусов.

2. Эвристический анализ - обнаружение вируса за счет отслеживания его последовательности действий. Обнаружение не известных вирусов.

3. Антивирусный мониторинг - обнаружение вирусов на “лету” за счет загрузки резидента антивирусной программы в оперативную память ПК.

4. Обнаружение изменений - обнаружение вирусов на основе предварительно полученных характеристик областей диска.

Виды антивирусных программ

1. Программы-фаги (сканеры).

Достоинства:

‑ обнаружение и удаление тела вируса;

‑ возможность резидентного функционирования;

‑ универсальность по типу обнаруживаемых вирусов.

Недостатки:

‑ относительно низкая скорость поиска;

‑ большой размер антивирусных баз;

‑ необходимость постоянной их актуализации.

2. Ревизоры дисков (CRC-сканеры).

Достоинства:

‑ Используют антистелс алгоритмы;

‑ обнаруживают вирус любого типа.

Недостатки:

‑ Не обнаруживают вирусы во вновь получаемых файлах (электронная почта, сменные носители и т.д.).

3. Программы-блокировщики.

Достоинства:

‑ обнаружение вируса на стадии загрузки;

‑ обнаруживают вирус любого типа.

Недостатки:

‑ не обеспечивают уничтожение вируса;

‑ психологическое воздействие на пользователя (назойливость).

4. Программы-иммунизаторы.

Достоинства:

‑ сообщают о “заражении” или блокируют его.

Недостатки:

‑ иммунизация от определенного типа вируса;

‑ сложность иммунизировать файлы от всех известных вирусов.