



Содержание :

- 1.Понятие вредоносного ПО
- 2.Классификация вредоносных программ
- 3.Признаки заражения
- 4.Основные типы вредоносных объектов
- 5. Способы защиты от вредоносных программ.

1. Понятие вредоносного ПО.

- К вредоносному программному обеспечению относятся сетевые черви, компьютерные вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие какой-либо вред компьютеру, на котором они запускаются, или другим компьютерам в сети.

2. Классификация вредоносных программ

**По среде обитания
(по поражаемым объектам)**

Файловые вирусы	Загрузочные вирусы	Сетевые вирусы	Макровирусы
Иницируются при запуске заражённой программы.	Записываются в загрузочный сектор диска и запускаются при запуске операционной системы	Самостоятельно копирует себя и распространяется по другим компьютерам, входящим в сеть	Поражают документы, выполненные в некоторых прикладных программах.

Классификация вредоносных программ

По алгоритмам работы

<i>Резидентные вирусы</i>	<i>Стелс-алгоритмы</i>	<i>Основанные на применении алгоритмов полиморфичности</i>
Загружаются в оперативную память, поэтому являются активными до полного выключения компьютера.	Перехватывает запрос ОС на чтение или запись зараженных объектов.	Не содержат ни одного постоянного участка кода, что достигается за счет шифрования кода вируса и модификации программы-расшифровщика



КЛАССИФИКАЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ

По деструктивным, то есть разрушительным возможностям

<i>Опасные вирусы</i>	<i>Неопасные вирусы</i>
Выводят из строя операционную систему, портят или уничтожают информацию, хранящуюся на диске.	Практически не влияют на работоспособность компьютера.

3. Признаки заражения

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM- устройства;
- произвольный запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой- либо из программ вашего компьютера выйти в интернет, хотя вы это никак не инициировали

4. Основные типы вредоносных объектов

Упаковщики	Трояны	Вредоносные утилиты	Adware	Информационные процессы, имеющие вредоносные последствия	
Архивируют содержимое файла	Маскируются под полезные программы	Автоматизация других вирусов, червей или троянских программ	Реклама	Спам	Фишинг

5. Способы защиты от вредоносных программ

Антивирусные сканеры	Антивирусные мониторы	Ревизоры изменений	Иммунизаторы	Поведенческие блокираторы
Просмотр всех файлов, загрузочных секторов и памяти с целью обнаружения в них вирусных сигнатур.	Фоновая проверка файлов, загрузочных секторов и памяти в реальном времени	Следит за изменениями файлов на компьютер	Сообщают о заражении, или блокируют.	Перехватывают различные события в системе.



Сетевые угрозы. Способы борьбы с сетевыми атаками