***Практическая работа № 15***

**Методы и средства защиты программ от компьютерных вирусов.**

*Цель работы:*  изучение способов применения методов и средств защиты

*Теоретическое обоснование*

Все имеющиеся на данный момент *методы* защиты компьютерных систем от программных закладок, в частности компьютерных вирусов, можно разделить на две группы:

1) *методы* *применения* *штатных защитных средств* компьютерной системы для построения и поддержания политики безопасности, адекватной в отношении защиты от программных закладок;

2) *методы* *применения специализированных антивирусных средств*, предназначенных для выявления, предупреждения и пресечения разрушающих воздействий на компьютерную систему со стороны программных закладок.

В настоящее время для борьбы с программными закладками в компьютерных системах применяют следующие *методы*:

* сканирование системы на предмет наличия известных программных закладок;
* контроль целостности программного обеспечения;
* контроль целостности конфигурации защищаемой системы;
* антивирусный мониторинг информационных потоков;
* создание ловушек и др.

Для защиты от компьютерных вирусов в настоящее время используются следующие *методы*:

|  |  |
| --- | --- |
| —           Архивирование.  —           Входной контроль.  —           Профилактика.  —           Ревизия.  —           Карантин. | —           Сегментация  —           Фильтрация.  —           Вакцинация.  —           Автоконтроль целостности.  —           Терапия. |

Для защиты от компьютерных вирусов в настоящее время используются следующие *средства*:

1. Профилактика. К профилактическим средствам относятся: перекрытие путей проникновения вирусов в компьютер; исключение возможности заражения и порчи вирусами, проникшими в компьютер, других файлов.
2. Диагностика. Диагностические средства позволяют обнаруживать вирусы в компьютере и распознавать их тип.
3. Лечение. Лечение состоит в удалении вирусов из зараженных программных средств и восстановлении пораженных файлов.

Основным средством борьбы с вирусом были и остаются антивирусные программы, использующие несколько основополагающих методик обнаружения и защиты от вирусов:

Сканирование — последовательный просмотр проверяемых файлов в поиске сигнатур известных вирусов. Используется только для поиска уже известных и изученных вирусов. Неэффективно для обнаружения шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора;

Эвристический анализ — обнаружение ранее неизвестных вирусов;

Использование антивирусных мониторов — автоматическая проверка всех запускаемых программ, создаваемых, открываемых и сохраняемых документов, файлов программ и документов, полученных через Интернет или скопированных на жесткий диск с дискеты или компакт-диска;

Обнаружение изменений — обнаружение изменений, внесенных в предварительно запомненные программой-ревизором характеристики всех областей диска;

Использование антивирусов, встроенных в BIOS компьютера — контроль обращений к главной загрузочной записи жестких дисков и к загрузочным секторам дисков и дискет.

Защитный комплекс основывается на применении антивирусных программ и проведении организационных мероприятий.

*Методические указания*

*Задания*

1. Повторите теоретический материал
2. Составьте перечень основных антивирусных методов
3. Проведите анализ методов.
4. Составьте перечень основных антивирусных средств

*Контрольные вопросы*

1. Назовите методы защиты компьютерных систем от программных закладок, в частности компьютерных вирусов
2. В чем заключается принцип использования этих методов
3. Назовите средства защиты
4. Дайте характеристику каждому из средств. Приведите примеры

*Форма отчёта*

Конспект, проверка письменной работы, ответы на вопросы