**Тема 3-4 Современные компьютерные угрозы и методы борьбы с ними**

**1. Что могут заразить вирусы?**

**Вирусы** действуют только программным путем. Они, как правило, присоединяются к файлу или проникают в тело файла. В этом случае говорят, что файл заражен вирусом. **Вирус** попадает в компьютер только вместе с зараженным файлом. Для активизации вируса нужно загрузить зараженный файл, и только после этого, вирус начинает действовать самостоятельно. Чаще всего **вирус** распространяется через зараженные диски, дискеты, флэшки, карты памяти мобильных телефонов, фотоаппаратов, видеокамер, электронную почту и интернет (скачивание программ).

**2. Как маскируются «невидимые» вирусы?**

Многие резидентные вирусы (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Такие вирусы называются невидимыми, или stealth (стелс) вирусами. Разумеется, эффект "невидимости" наблюдается толькона зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

**3. Каковы особенности самомодифицирующихся вирусов?**

Самомодифицирующиеся вирусы (мутанты) изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.

**4. Какие методы защиты от компьютерных вирусов можно использовать?**

Для защиты от вирусов можно использовать:

* Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
* профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
* специализированные программы для защиты от вирусов.

**5. В каких случаях применяют специализированные программы защиты от компьютерных вирусов?**

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

**6. На какие виды можно подразделить программы защиты от компьютерных вирусов?**

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов:

* Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
* Программы-доктора, или фаги, восстанавливают зараженные программы убирая из них тело вируса, т.е. программа возвращается в то состояние, в котором она находилась до заражения вирусом.
* Программы-ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.
* Доктора-ревизоры – это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
* Программы-фильтры располагаются резидентно в оперативной памяти компьютера, перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

**7. Как действуют программы-детекторы?**

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Программа Scan фирмы McAfee Associates и Aidstest Д.Н.Лозинского позволяют обнаруживать около 9000 вирусов, но всего их более двадцати тысяч! Некоторые программы-детекторы, например Norton AntiVirus или AVSP фирмы "Диалог-МГУ", могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не мнение невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

**8. Что называется сигнатурой?**

Сигнатура вируса - это уникальная последовательность байтов, принадлежащая вирусу и не встречающаяся в других программах.

**9. Всегда ли детектор распознает зараженную программу?**

Использование программ-сканеров не защищает компьютер от новых вирусов. Кроме того, такие программы не могут обнаружить большинство полиморфных вирусов, так как для таких вирусов невозможно определить сигнатуру. В последнее время программы-детекторы поставляются со специальными базами данных - сигнатурами вирусов, которые может пополнять сам пользователь. Некоторые сканеры позволяют подключать к своей базе данных внешние файлы - дополнения, содержащие сведения о новых вирусах. В таких случаях достаточно приобретать новые файлы-дополнения к базе для обновления антивирусной программы.

**10. Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?**

**Программы-ревизоры** первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, параметры всех контролируемых файлов (иногда только контрольную сумму файлов), информацию о структуре каталогов, номера плохих кластеров диска, иногда - объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры и многое другое.

Существуют также **программы-фильтры**, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

**Программы-вакцины**, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

**11.Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?**

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов

**12. Перечислите меры защиты информации от компьютерных вирусов.**

Основным средством защиты информации является **резервное копирование** наиболее ценных данных. В случае утраты информации жесткие диски переформатируются и подготавливают к новой эксплуатации. На “чистый” отформатированный диск устанавливают все необходимое программное обеспечение, которое тоже берут с дистрибутивных носителей. Восстановление компьютера завершается восстановлением данных, которые берут с резервных носителей.

Вспомогательными средствами защиты информации являются **антивирусные программы и средства аппаратной защиты.**

**13. Каковы современные технологии антивирусной защиты?**

Технология антивирусной защиты представляет собой совокупность методов обнаружения и удаления программных компонентов, несанкционированно внедрённых в информационную сферу АС и предназначенных для выполнения несанкционированных действий, направленных на реализацию угроз ИБ. Такие программные компоненты принято называть «вирусами» [46]. Частными случаями вирусов являются: информационные «закладки», информационные люки, программы типа «троянский конь» и др. Внесение вирусов может осуществляться нарушителем как на техноло-гическом, так и на эксплуатационном этапе жизненного цикла ГСПД.

Технология антивирусной защиты реализуется при помощи специализированного программного обеспечения, называемого антивирусными программами. Существует четыре основных типа антивирусных программ: сканеры, программы контроля целостности данных, мониторы и гибридные антивирусные средства.