**Вопрос 1**

**Понятие о компьютерной безопасности**

В вычислительной технике понятие безопасности является весьма широким. Оно

подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту

информации от внесения в нее изменений неуполномоченными лицами, и сохранение

тайны переписки при электронной связи. Разумеется, во всех цивилизованных

странах на страже безопасности граждан стоят законы, но в сфере

вычислительной техники правоприменительная практика пока развита недостаточно,

а законотворческий процесс не успевает за развитием технологий, поэтому надежность

работы компьютерных систем во многом опирается на меры самозащиты.

**Компьютерные вирусы**

Компьютерный вирус — это программный код, встроенный в другую программу,

или в документ, или в определенные области носителя данных и предназначенный

для выполнения несанкционированных действий на несущем компьютере.

Основными типами компьютерных вирусов являются:

• программные вирусы;

• загрузочные вирусы;

• макровирусы.

К компьютерным вирусам примыкают и так называемые *троянские кони {троянские*

*программы, троянцы).*

**Программные вирусы.** Программные вирусы — это блоки программного кода, целенаправленно

внедренные внутрь других прикладных программ. При запуске программы,

несущей вирус, происходит запуск имплантированного в нее вирусного

кода. Работа этого кода вызывает скрытые от пользователя изменения в файловой

системе жестких дисков и/или в содержании других программ. Так, например,

вирусный код может воспроизводить себя в теле других программ — этот процесс

*K2L3biB2ieTCH размножением.* По прошествии определенного времени, создав достаточное

количество копий, программный вирус может перейти к разрушительным

действиям — нарушению работы программ и операционной системы, удалению

информации, хранящейся на жестком диске. Этот процесс называется *вирусной*

*атакой.*

Самые разрушительные вирусы могут инициировать форматирование жестких

дисков. Поскольку форматирование диска — достаточно продолжительный процесс,

который не должен пройти незамеченным со стороны пользователя, во многих

случаях программные вирусы ограничиваются уничтожением данных только

в системных секторах жесткого диска, что эквивалентно потере таблиц файловой

струюуры. В этом случае данные на жестком диске остаются нетронутыми, но воспользоваться

ими без применения специальных средств нельзя, поскольку неизвестно,

какие сектора диска каким файлам принадлежит. Теоретически восстановить данные

в этом случае можно, но трудоемкость этих работ исключительно высока.

Считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение

компьютера. Однако бывают случаи, когда аппаратное и программное обеспечение

настолько взаимосвязаны, что программные повреждения приходится

устранять заменой аппаратных средств. Так, например, в большинстве современных

материнских плат базовая система ввода-вывода *(BIOS)* хранится в перезаписываемых

постоянных запоминающих устройствах (так называемая *флэш-память).*

Возможность перезаписи информации в микросхеме флэш-памяти используют

некоторые программные вирусы для уничтожения данных *BIOS.* В этом случае

для восртановления работоспособности компьютера требуется либо замена микросхемы,

хранящей *BIOS,* либо ее перепрограммирование на специальных устройствах,

называемых *программаторами*

Программные вирусы поступают на компьютер при запуске непроверенных программ,

полученных на внешнем носителе (гибкий диск, компакт-диск и т. п.) или

принятых из Интернета. Особое внимание следует обратить на слова *при запуске.*

При обычном копировании зараженных файлов заражение компьютера произойти

не может. В связи с этим все данные, принятые из Интернета, должны проходить

обязательную проверку на безопасность, а если получены незатребованные данные

из незнакомого источника, их следует уничтожать, не рассматривая. Обычный

прием распространения «троянских» программ — приложение к электронному

письму с «рекомендацией» извлечь и запустить якобы полезную программу.

Загрузочные вирусы. От программных вирусов загрузочные вирусы отличаются

методом распространения. Они поражают не программные файлы, а определенные

системные области магнитных носителей (гибких и жестких дисков). Кроме того,

на включенном компьютере они могут временно располагаться в оперативной памяти.

Обычно заражение происходит при попытке загрузки компьютера с магнитного

носителя, системная область которого содержит загрузочный вирус. Так, например,

при попытке загрузить компьютер с гибкого диска происходит сначала проникновение

вируса в оперативную память, а затем в загрузочный сектор жестких дисков.

Далее этот компьютер сам становится источником распространения загрузочного

вируса.

Макровирусы. Эта особая разновидность вирусов поражает документы, выполненные

в некоторых прикладных программах, имеющих средства для исполнения так

*^2i3biBcieubix макрокоманд.* В частности, к таким документам относятся документы

текстового процессора *Microsoft Word* (они имеют расширение .DOC). Заражение

происходит при открытии файла документа в окне программы, если в ней не отключена

возможность исполнения макрокоманд. Как и для других типов вирусов, результат

атаки может быть как относительно безобидным, так и разрушительным.

**Методы защиты от компьютерных вирусов**

Существуют три рубежа защиты от компьютерных вирусов:

• предотвращение поступления вирусов;

• предотвращение вирусной атаки, если вирус все-таки поступил на компьютер;

• предотвращение разрушительных последствий, если атака все-таки произошла.

Существуют три метода реализации защиты:

• программные методы защиты;

• аппаратные методы защиты;

• организационные методы защиты.

В вопросе защиты ценных данных часто используют бытовой подход: «болезнь

лучше предотвратить, чем лечить». К сожалению, именно он и вызывает наиболее

разрушительные последствия. Создав бастионы на пути проникновения вирусов в

компьютер, нельзя положиться на их прочность и остаться неготовым к действиям

после разрушительной атаки. К тому же вирусная атака — далеко не единственная

и даже не самая распространенная причина утраты важных данных. Существуют

программные сбои, которые могут вывести из строя операционную систему, а также

аппаратные сбои, способные сделать жесткий диск неработоспособным. Всегда

существует вероятность утраты компьютера вместе с ценными данными в результате

кражи, пожара или иного стихийного бедствия.

Поэтому создавать систему безопасности следует в первую очередь «с конца» —

с предотвращения разрушительных последствий любого воздействия, будь то

вирусная атака, кража в помещении или физический выход жесткого диска из строя.

Надежная и безопасная работа с данными достигается только тогда, когда любое

неожиданное событие, в том числе и полное физическое уничтожение компьютера,

не приведет к катастрофическим последствиям.