8.8. Защита от компьютерных вирусов

Имеющиеся в настоящее время средства противодействия компьютерным вирусам достаточны для того, чтобы предотвратить серьезный ущерб от их воздействия. Однако это возможно только при внимательном отношении к данной проблеме. За последнее время большинство вирусных эпидемий возникало в среде малоквалифицированных пользователей.

Для противодействия компьютерным вирусам и другим типам вредоносных программ в ИТ применяется комплекс мер и средств защиты, среди которых можно выделить следующие виды,

1. **Юридические меры защиты от компьютерных вирусов.**

   Для успешной борьбы с распространением вирусов и других типов вредоносных программ в нашей стране необходимо совершенствовать отечественное законодательство в этой области.

2. **Административные и организационные меры защиты** от компьютерных вирусов на современном этапе являются более действенными. Они заключаются в составлении четких планов профилактических мероприятий и планов действия на случай возникновения заражений.

   В подразделениях предприятий и организаций, связанных с эксплуатацией (использованием) программного обеспечения, применяются более жесткие административные и организационные меры по сравнению с подразделениями, занятыми разработкой приложений и прикладных программных продуктов для ИТ. Это чаще всего оказывается возможным, т. к. в эксплуатирующих подразделениях предприятий и организаций собственная разработка программного обеспечения не производится и все новые программы они получают от разработчиков или вышестоящих организаций через специальные подразделения, адаптирующие программные средства к реальным условиям экономического объекта.

   С другой стороны, наличие вируса, "троянского коня" или другой вредоносной программы в ИТ зачастую приводит к гораздо более тяжелым последствиям, т. к. они имеют дело с реальной экономической, производственной или иной информацией.

   Для подразделений, занятых разработкой специальных вспомогательных программ, по сравнению с эксплуатирующими, административные и организационные меры должны быть более мягкими. Платой за чрезмерное администрирование является существенное снижение темпов и качества разработки программных продуктов.

   Возможны четыре способа проникновения вируса или другого типа вредоносной программы в эксплуатируемую систему:

   - вирус или другая вредоносная программа поступает вместе с программным обеспечением, предназначенным для последующего использования в работе;

- вирус или другой тип вредоносной программы поступает в систему при приеме сообщений по сети;
- вирус или другая вредоносная программа приносятся персоналом с программами, не относящимися к эксплуатируемой системе;
- вирус или другой тип вредоносной программы преднамеренно создаются обслуживающим персоналом.

Источник вируса легко выявляется, если в эксплуатируемой ИТ производится разграничение доступа пользователей к привилегированным функциям и оборудованию, присутствуют надежные средства регистрации процесса всего технологического цикла, включая регистрацию внутримашинных процессов. Особенно важными являются меры разграничения доступа в вычислительных сетях.

3. **Программно-аппаратные меры защиты** основаны на использовании программных антивирусных средств и специальных аппаратных средств (специальных плат), с помощью которых производится контроль зараженности вычислительной системы, контроль доступа, шифрование данных и регистрация попыток обращения к данным.

Наиболее часто в ИТ используются два метода защиты от вирусов с помощью использования специального программного обеспечения:

1. Применение "иммуностойких" программных средств, защищенных от возможности несанкционированной модификации (разграничение доступа, методы самоконтроля и самовосстановления).
2. Применение специальных антивирусных программных средств, осуществляющих:
   - постоянный контроль возникновения отклонений в деятельности прикладных программ;
   - периодическую проверку наличия других возможных следов вирусной активности (например, обнаружение нарушений целостности программного обеспечения);
   - входной контроль новых программ и файлов перед их использованием (по характерным признакам наличия в их теле вирусных образований);
   - удаление вирусов и по возможности восстановление пораженных файлов.

В настоящее время на рынке программных продуктов имеется довольно большое число специальных антивирусных программ. В основе работы большинства их лежит принцип поиска сигнатуры вирусов.

Обычно в антивирусные программы входит периодически обновляемая база данных сигнатур вирусов. Антивирусная программа просматривает компьютерную систему, проводя сравнение и отыскивая соответствие с сигнатурами в базе данных. Когда программа находит соответствие, она пытается убрать обнаруженный вирус.

По методу работы антивирусные программы подразделяются на следующие основные виды,

1. **Вирус-фильтр (сторож)** - это резидентная программа, обнаруживающая свойственные для вирусов действия и требующая от пользователя подтверждения на их выполнение. В качестве проверяемых действий выступают:
   - обновление программных файлов и системной области диска;

- форматирование диска;
- резидентное размещение программы в оперативной памяти и т. д.

Пользователь в ответ на это должен либо разрешить выполнение действия, либо запретить его. Подобная часто повторяющаяся "назойливость", раздражающая пользователя, и то, что объем оперативной памяти уменьшается из-за необходимости постоянного нахождения в ней вирус-фильтра, являются главными недостатками этих программ. К тому же эти программы не лечат файлы или диски, для этого необходимо использовать другие антивирусные программы.

Однако вирус-фильтры позволяют обеспечить определенный уровень защиты персонального компьютера от деструктивных действий вирусов.

2. **Детектор (сканер)** - это специальные программы, предназначенные для просмотра всех возможных мест нахождения вирусов (файлы, операционная система, внутренняя память и т. д.) и сигнализирующие об их наличии.
3. **Дезинфектор (доктор)** - это программа, осуществляющая удаление вируса из программного файла или памяти ПК. Если это возможно, то дезинфектор восстанавливает нормальное функционирование ПК. Однако ряд вирусов искажает систему так, что ее исходное состояние дезинфектор восстановить не может.
4. **Программы-вакцины**, или иммунизаторы, относятся к резидентным программам. Они модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них.
5. **Полидетектор-дезинфектор** - это интегрированные программы, позволяющие выявить вирусы в персональном компьютере, обезвредить их и по возможности восстановить пораженные файлы и программы. В некоторых случаях программы этого семейства позволяют блокировать зараженный файл от открытия и перезаписи.

Однако, несмотря на все меры антивирусной защиты, стопроцентной гарантии от вирусов в настоящее время не существует.

Поэтому в целях защиты информационной технологии от компьютерных вирусов необходимо соблюдать следующие правила:

Правило первое. Следует осторожно относиться к программам и документам, полученным из глобальных сетей. Перед тем, как запустить файл на выполнение или открыть документ, базу данных и прочее, необходимо в обязательном порядке проверить их на наличие вирусов.

Правило второе. Для уменьшения риска заразить файл на сервере локальной вычислительной сети следует активно использовать стандартные возможности защиты сетей:

- ограничение прав пользователей;
- установку атрибутов "только для чтения" или "только на запуск" для выполняемых файлов;
- скрытие (закрытие) важных разделов диска и директорий.

В локальных вычислительных сетях следует использовать специализированные антивирусные средства, проверяющие все файлы, к которым идет обращение. Если это по

каким-либо причинам невозможно, необходимо регулярно проверять сервер обычными антивирусными средствами. Необходимо также перед тем, как запустить новое программное обеспечение, проверить его на тестовом персональном компьютере, не подключенном к общей сети.

Правило третье. Следует приобретать дистрибутивные копии программных продуктов у официальных поставщиков. При этом значительно снижается вероятность заражения.

Правило четвертое. Следует хранить дистрибутивные копии программного обеспечения (в том числе копии операционной системы), причем копии желательно хранить на защищенных от записи машинных носителях.

Следует пользоваться только хорошо зарекомендовавшими себя источниками программного обеспечения.

Правило пятое. Не следует запускать непроверенные файлы, в том числе полученные из компьютерной сети. Желательно использовать только программы, полученные из надежных источников. Перед запуском новых программ обязательно следует проверять их одним или несколькими антивирусными средствами.

Правило шестое. Необходимо пользоваться утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах. Следует периодически сравнивать информацию, хранящуюся в подобной базе данных, с информацией, записанной на винчестере. Любое несоответствие может служить сигналом о появлении вируса.

Правило седьмое. Следует периодически сохранять на внешнем носителе файлы, с которыми ведется работа.

Для эффективности защиты информации от компьютерных вирусов необходимо использовать комплекс всех известных способов и средств, выполняя мероприятия непрерывно.

Практическое задание

Разработайте и приведите графическое изображение схемы технологического процесса обработки информации на одном из ниже перечисленных экономических объектов:

- торговой организации;
- образовательного учреждения;
- филиала банка;
- налоговой инспекции;
- страховой организации;
- производственного предприятия;
- бухгалтерии учреждения.

Практическое задание

Задание 1

Отправьте по электронной почте данные по производственной задаче: сведения о заказах фирмы ОАО "Винчестер", представленные в таблице.

Сведения о заказах фирмы ОАО "Винчестер"			
Месяц	**Наименование товара**	**Объемы заказа, шт.**	**Количество заказов**
Январь	ПК	75	10
Февраль	Ноутбук	80	12
Март	ПК	62	8
Апрель	ПК	52	9
Май	ПК	48	10
Июнь	ПК	20	5
Июль	ПК	10	6
Август	Ноутбук	15	7
Сентябрь	Ноутбук	95	15
Октябрь	ПК	82	10
Ноябрь	ПК	100	20
Декабрь	ПК	110	21

Задание 2

С помощью электронной почты отправьте информацию, представленную в графическом виде (гистограмма, диаграмма или график), используя данные задания 1.