8.6. Понятие и виды вредоносных программ

Первые сообщения о несущих вред программах, преднамеренно и скрытно внедряемых в программное обеспечение различных вычислительных систем, появились в начале 80-х гг. Название "компьютерные вирусы" произошло, вероятно, по причине сходства с биологическим прототипом, с точки зрения возможности самостоятельного размножения. В новую компьютерную область были перенесены и некоторые другие медико-биологические термины, например такие, как мутация, штамм, вакцина и др.

Сообщение о программах, которые при наступлении определенных условий начинают производить вредные действия, например, после определенного числа запусков разрушают хранящуюся в системе информацию, но при этом не обладают характерной для вирусов способностью к самовоспроизведению, появились значительно раньше. По аналогии с персонажем известного древнегреческого мифа такие программы получили название "троянских коней".

Кроме таких программ в настоящее время выделяют целый ряд разновидностей вредоносных программ и компьютерных вирусов, которые являются существенной угрозой безопасности информации в информационных технологиях.

Выделяют следующие классы вредоносных программ, включая компьютерные вирусы,

1. **Люк.** Условием, способствующим реализации многих видов угроз безопасности информации в информационных технологиях, является наличие "люков".

   Люк вставляется в программу обычно на этапе отладки для облегчения работы: данный модуль можно вызывать в разных местах, что позволяет отлаживать отдельные части программы независимо.

   Наличие люка позволяет вызывать программу нестандартным образом, что может отразиться на состоянии системы защиты. Люки могут остаться в программе по разным причинам:

   - их могли забыть убрать;
   - оставили для дальнейшей отладки;
   - оставили для обеспечения поддержки готовой программы;
   - оставили для реализации тайного доступа к данной программе после ее установки.

   Большая опасность люков компенсируется высокой сложностью их обнаружения (если, конечно, не знать заранее об их наличии), т. к. обнаружение люков - результат случайного и трудоемкого поиска. Защита от люков одна - не допускать их появления в программе, а при приемке программных продуктов, разработанных другими производителями, следует проводить анализ исходных текстов программ с целью обнаружения люков.

2. **Логические бомбы**, как вытекает из названия, используются для искажения или уничтожения информации, реже с их помощью совершаются кража или мошенничество. Логическую бомбу иногда вставляют во время разработки

программы, а срабатывает она при выполнении некоторого условия (время, дата, кодовое слово).

Манипуляциями с логическими бомбами занимаются также чем-то недовольные служащие, собирающиеся покинуть организацию, но это могут быть и консультанты, служащие с определенными политическими убеждениями и т. п.

Реальный пример логической бомбы: программист, предвидя свое увольнение, вносит в программу расчета заработной платы определенные изменения, которые начинают действовать, когда его фамилия исчезнет из набора данных о персонале фирмы.

3. **Троянский конь** - программа, выполняющая в дополнение к основным, т. е. запроектированным и документированным действиям, действия дополнительные, не описанные в документации. Аналогия с древнегреческим троянским конем оправданна - и в том и в другом случае в не вызывающей подозрения оболочке таится угроза. Троянский конь представляет собой дополнительный блок команд, тем или иным образом вставленный в исходную безвредную программу, которая затем передается (дарится, продается, подменяется) пользователям ИТ. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени, по команде извне и т. д.). Запустивший такую программу подвергает опасности как свои файлы, так и всю ИТ в целом. Троянский конь действует обычно в рамках полномочий одного пользователя, но в интересах другого пользователя или вообще постороннего человека, личность которого установить порой невозможно.

   Наиболее опасные действия троянский конь может выполнять, если запустивший его пользователь обладает расширенным набором привилегий. В таком случае злоумышленник, составивший и внедривший троянского коня и сам этими привилегиями не обладающий, может выполнять несанкционированные привилегированные функции чужими руками.

   Для защиты от этой угрозы желательно, чтобы привилегированные и непривилегированные пользователи работали с различными экземплярами прикладных программ, которые должны храниться и защищаться индивидуально. А радикальным способом защиты от этой угрозы является создание замкнутой среды использования программ.

4. **Червь** - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе.

   Червь использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий. Наиболее известный представитель этого класса - вирус Морриса (червь Морриса), поразивший сеть Internet в 1988 г. Подходящей средой распространения червя является сеть, все пользователи которой считаются дружественными и доверяют друг другу, а защитные механизмы отсутствуют. Наилучший способ защиты от червя - принятие мер предосторожности против несанкционированного доступа к сети.

5. **Захватчик паролей** - это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к рабочей станции

информационной технологии на экран выводится информация, необходимая для окончания сеанса работы. Пытаясь организовать вход, пользователь вводит имя и пароль, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке, а ввод и управление возвращаются к операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля возможен и другими способами. Для предотвращения этой угрозы перед входом в систему необходимо убедиться, что вы вводите имя и пароль именно системной программе ввода, а не какой-нибудь другой. Кроме того, необходимо неукоснительно придерживаться правил использования паролей и работы с системой. Большинство нарушений происходит не из-за хитроумных атак, а из-за элементарной небрежности. Соблюдение специально разработанных правил использования паролей - необходимое условие надежной защиты.

6. **Бактерии (bacteria).** Этот термин вошел в употребление недавно и обозначает программу, которая делает копии самой себя и становится паразитом, перегружая память и микропроцессор персонального компьютера или рабочей станции сети.
7. **Компьютерным вирусом** принято называть специально написанную, обычно небольшую по размерам программу, способную самопроизвольно присоединяться к другим программам (т. е. заражать их), создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в файлы, системные области персонального компьютера и в другие объединенные с ним компьютеры с целью нарушения нормальной работы программ, порчи файлов и каталогов, создания различных помех при работе на компьютере.