Глоссарий

Антивирусная программа - Программа, предназначенная для предотвращения доступа к персональному компьютеру для вредоносных программ — она обнаруживает инфицированные файлы и удаляет их.

Брандмауэр - Программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельной компьютерной системой. Например, брандмауэр позволяет ограничивать трафик на основе предварительно заданных правил, которые разрешают обмен данными только между указанными адресами.

Вирус - Вредоносная программа, которая распространяется, копируя себя в другие программы. Вирус может распространяться через файлы, сообщения электронной почты или веб-страницы. Компьютер может заразиться вирусом во время работы пользователя в Интернете или при открытии вложений электронной почты. Вирусы могут снизить работоспособность компьютера или системы.

Всплывающее окно - Новое окно, которое открывается поверх активного окна обозревателя Интернета. Как правило, такое окно не содержит собственного веб-адреса, однако в некоторых случаях может его содержать. Во всплывающих окнах, которые открываются без запроса пользователя, обычно содержится реклама.

Дискуссионный форум - Место обсуждения в Интернете, часто посвященное определенной теме. Здесь люди могут оставлять сообщения в интерактивном режиме, используя форматы, указанные поставщиком данной услуги. Для некоторых дискуссионных форумов требуется регистрация.

В некоторых форумах имеется архив, который можно использовать для поиска определенной темы. Некоторые форумы контролируются администратором, который имеет право удалять и редактировать любые размещенные сообщения или запрещать доступ для пользователей, которые оскорбляют своих собеседников.

Загрузка -Сохранение файлов из Интернета на собственном компьютере.

Защита данных - Набор правил, которые обеспечивают сохранение конфиденциальности информации. Безопасность данных распространяется на конфиденциальную информацию, например, личную информацию, и поддерживается политикой информационной безопасности или заявлением о конфиденциальной информации.

Информационная безопасность- Политика, реализуемая для обеспечения контроля над рисками информационной безопасности.

Операционная система - Главная программа, которая работает «между» компьютером и прикладным программным обеспечением. С помощью операционной системы компьютер управляет установленным программным обеспечением, а также контролирует и использует его. К распространенным операционным системам относятся Microsoft® Windows®, Apple® Mac OS и Linux®.

Опасные программы: вирусы, черви и трояны Программа или часть программы, которая предназначена для распространения нежелательных событий в компьютерной или информационной системе, например, вирусов, червей или троянов.

Почта; электронная почта; сообщение электронной почты - Электронная передача текста или изображений между адресами компьютерного приложения.

Сервер - Программа, которая распределяет файлы по компьютерам в сети на основе предварительно заданных правил. Например, в Интернете пользователи получают сообщения электронной почты от сервера электронной почты сети. Сервером часто называют компьютер, на котором установлена серверная программа.

Сетевой дневник - Общественный интерактивный дневник.

Спам - Нежелательная электронная почта, которая, как правило, рассылается в целях прямого почтового маркетинга. Спам почти всегда единовременно рассылается большому кругу получателей.

Хакер, взломщик Человек, взламывающий информационные сети или системы организации, либо использующий их без разрешения. Примечание: термин «хакер» имеет два значения — он может также означать опытного компьютерного пользователя. (см. Хакеры и взломщики)

Чат -Дискуссионный форум, работающий в режиме реального времени. В нем пользователи поочередно пишут сообщения, сразу отображающиеся на экране. Сообщения заменяются по мере написания новых, поэтому отображаются только самые последние сообщения.

Червь - Вредоносная программа, которая может независимо распространяться через информационные сети. Черви могут распространяться через электронную почту или бреши в системе защиты информации в обозревателе Интернета или операционной системе. Даже если пользователем не выполняются никакие действия, черви могут получить доступ к незащищенным компьютерам при их подключении к Интернету. Черви затрудняют работу системы или компьютера и могут распространять другие вредоносные программы.