УДК 004.7.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ

Рула Д. Д., студ.
(ГОУ ВПО «Донецкий национальный технический университет», г. Донецк, ДНР)

На сегодняшний день компьютерная сеть является привычной программа, а также инструментом для обмена информацией. В связи с созданием компьютерных сетей с многопользовательским доступом в локальных и глобальных сетях возникает ряд взаимосвязанных проблем защиты информации, хранящихся на компьютерах или серверах компьютерной сети. Современные сетевые операционные системы, которые уже полностью защищены от атак и угроз, также представляют собой мощное средство защиты от несанкционированного доступа к сетевым ресурсам. Однако случаются ситуации, когда такая защита становится уязвимой, и программные продукты не работают для защиты информации. Практика показывает, что несанкционированный пользователь или программные продукты, называемые вирусами с достаточным опытом в области системного и сетевого программирования, назначенные для подключения к сети, даже для ограниченного доступа к отдельным ресурсам, рано или поздно могут получить доступ к некоторым защищенным ресурсам сети. Поэтому существует проблема с дополнительным аппаратным и программным обеспечением для защиты сетевых ресурсов от несанкционированного доступа или соединения.

К аппаратной защите различных брандмауэров, брандмауэров, фильтров, антивирусных программ, устройств шифрования протоколов и т. д.

Средства защиты программного обеспечения включают в себя: соединения сетевого мониторинга (мониторинг сети); инструменты архивации данных; антивирусные программы; криптографические средства; средства идентификации и аутентификации пользователей; контроль доступа; регистрации и аудита [1].

В качестве примеров сочетаний вышеуказанных мер можно привести:

- защита баз данных;
- защита информации при работе в компьютерных сетях.

При создании крупномасштабных (локальных, корпоративных и т. д.) компьютерных сетей возникает проблема обеспечения взаимодействия большого количества компьютеров, серверов, подсетей и сетей, т. Е. Проблема поиска и выбора оптимальных топологий становится основной задачей. Самым важным компонентом локальных и корпоративных сетей является их топология системы, которая определяется архитектурой межкомпьютерных коммуникаций.

Известно, что критическая информация должна обрабатываться в компьютерных сетях для обеспечения безопасности информации и сети. Термин «критическая информация»: некоторые факты о намерениях, способностях и действиях, жизненно важных для эффективного управления и функционирования критических структур, эффективного выполнения стоящих стратегических задач с различными грифами секретности; информация для служебного пользования; информация, составляющая коммерческую тайну или секрет фирмы; информация, которая является собственностью какой-либо организации или отдельного лица [2].

В компьютерных сетях должны быть предусмотрены аутентификация и шифрование, но данные элементы защиты не всегда обеспечивают надежную безопасность сети:

1. Применение шифрования в разы уменьшает скорость передачи данных по каналу, поэтому, довольно часто, шифрование сознательно не применяется системными администраторами для оптимизации трафика;

2. В компьютерных сетях чаще всего используются устаревшие технологии шифрования, которые, с помощью некоторых программ, можно очень быстро взломать и получить доступ в сеть.

Каждый узел сети является самостоятельной компьютерной системой. С точки зрения безопасности компьютерные сети обладают следующими недостатками:

— недостаточный контроль над клиентскими компьютерами;

— отсутствие механизма разграничения доступа нескольких пользователей к разным ресурсам на одном компьютере;

— необходимость подготовленности пользователя к различным административным мерам — обновлению антивирусной базы, архивированию данных, определению механизмов доступа к раздаваемым ресурсам и т. д.;

— разделение ресурсов и загрузка распределяются по различным узлам сети, многие пользователи имеют потенциальную возможность доступа к сети как к единой компьютерной системе;

— неопределенная периферия сильно влияет на возможность определения точных пределов сети. Один и тот же узел может одновременно работать в нескольких сетях, и, следовательно, ресурсы одной сети вполне могут использоваться с узлов, входящих в другую сеть;

— неопределённое распределение траектории доступа. Пользователь или захватчик может затребовать доступ к ресурсам некоторого узла сети, с которым данный узел не связан напрямую сетью. В таких случаях доступ осуществляется через некоторый промежуточный узел, связанный с обоими узлами, или даже через несколько промежуточных узлов. В компьютерных сетях весьма непросто точно определить, откуда именно пришел запрос на доступ, особенно если захватчик попытается скрыть это;

— слабая защищенность линии связи. Сеть тем и отличается от отдельной системы, что непременно включает в себя линии связи, по которым между узлами передаются данные. Это может быть элементарный провод, а может быть линия радиосвязи, в том числе и спутниковый канал. При наличии определенных условий (и соответствующей аппаратуры) к проводу можно незаметно (или почти незаметно) подсоединиться, радиолинию можно успешно прослушивать — т. е. ничто не препятствует тому, чтобы «выкачивать» передаваемые сообщения из линий связи и затем выделять из всего потока требуемые. [3]

На основе анализа угрозы безопасности компьютерных сетей можно сделать выводы о свойствах и функциях, которые должна обладать система обеспечения безопасности локальных и корпоративный сетей (КС).

1. Идентификация защищаемых ресурсов, т. е. при подключении к компьютерным сетям присвоение защищаемым ресурсам идентификаторов, по которым в дальнейшем система производит аутентификацию.
2. Аутентификация защищаемых ресурсов.
3. Применение парольной защиты ресурсов во всей части компьютерной сети.
4. Регистрация всех действий: вход пользователя в сеть, выход из сети, нарушение прав доступа к защищаемым ресурсам и т. д.
5. Обеспечение защиты информации при проведении сканирование сети от вредоносных программ и во время ремонтно-профилактических работ.

Перечень ссылок

1. Варлатая, С. К. «Защита информационных процессов в компьютерных сетях.» Учебно-методический комплекс / С. К. Варлатая, М. В. Шаханова. - Москва : Проспект, 2015. -216 с.

2. Вишневский, В. М. Теоретические основы проектирования компьютерных сетей / В. М. Вишневский. – Москва : Техносфера, 2003. – 512 с.

3. Шамова, Т. И. Управление образовательным процессом в адаптивной школе / Т. И. Шамова, Т. М. Давыденко – Москва : Центр, 2001. - 384 с.