Малышева Юлия Николаевна

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Распределенные автоматизированные системы

Анализ политики информационной безопасности

Аннотация. В статье рассматриваются проблемы информационной безопасности компьютерных сетей и основные функции системы защиты информации.

Ключевые слова: информационные технологии, информационная безопасность, автоматизированные средства безопасности, информация, локальная сеть.

В связи с «многопользовательским» режимом работы в компьютерной сети существует ряд взаимосвязанных проблем в защите информации, хранящейся на компьютерах или серверах компьютерной сети [1; 2].

Следует отметить, что сетевые операционные системы обеспечивают мощные функции безопасности для предотвращения несанкционированного доступа к сетевым ресурсам. Все же часто случаются случаи, когда даже подобная защита не работает.

Практика показывает, что неавторизованные пользователи с большим опытом программирования сетевых систем, которые пытаются подключиться к сети даже с ограниченным доступом к определенным ресурсам, рано или поздно все равно могут получить доступ к некоторым защищенным сетям, которые ее поддерживают.

Вследствие этого необходимо организовать дополнительное программное и аппаратное обеспечение для защиты сетевых ресурсов. Функции аппаратной

безопасности включают различные брандмауэры, фильтры, устройства шифрования протоколов и многое другое.

Средства защиты программного обеспечения включают: программы, которые шифруют данные, программы, которые отслеживают сетевые подключения (мониторинг сети); программы аутентификации и идентификации и т. д. [5]. Если вы разрабатываете глобальную компьютерную сеть с проблемами, которые обеспечивают согласованность огромного количества серверов, компьютер задается вопросом о поиске наилучшей поддержки топологии.

Существенным компонентом корпоративных и локальных сетей является их системная топология, которая определяется архитектурой соединений между компьютерами [3; 4].

Конечно, важная информация должна обрабатываться компьютерными сетями для обеспечения безопасности.

Термин «конфиденциальная информация» означает следующую информацию: различные указания на безопасность; информацию об официальном использовании информации, составляющей корпоративную тайну, и коммерческую конфиденциальную информацию – такую, как активы физических лиц и организаций.

Типичные уязвимые места компьютерных сетей:

1) кража итогов выдачи,
2) неразрешенное подключение,
3) неправильная работа линии связи,
4) неправильная работа пользователя,
5) кража внешних носителей информации [1].

Поскольку информация и загрузка материалов осуществляются через различные сетевые узлы, несколько пользователей могут получить доступ к сети одной компьютерной системы [2].

Сложность системы – получив доступ к одной из систем, входящих в сеть, пользователь (или захватчик) имеет реальную возможность атаковать

другие системы сети, другие компьютерные системы, необходимые для операционной системы, которая создает структурные компоненты программы. В связи с этим важно установить четкие требования к безопасности, особенно к сети общего назначения, которая развивалась без учета безопасности [6].

Полезные сайты сильно влияют на невозможность в большинстве случаев определить их точные границы. Один и тот же узел может непрерывно работать с этими сайтами, и, следовательно, информация в Интернете может с таким же успехом использовать среду, ограниченную узлами, принадлежащими другому веб-сайту.

Такое масштабное разделение ресурсов, несомненно, является преимуществом. Однако неопределенное количество потенциально неподготовленных пользователей и потенциальных захватчиков значительно усложняет безопасность как сети в целом, так и большинства ее отдельных узлов, создавая множественность точек атаки.

Компьютерной системе необходимо контролировать доступ к системе пользователя, так как этот доступ осуществляется из их текущего посещения.

Проблема в Интернете совершенно иная: так называемый удаленный доступ из одного и того же сетевого узла может запрашивать разные файлы. Таким образом, если человек одной и той же системы может проводить четкую политику безопасности в отношении своего вала, то президент сетевых узлов не имеет таких знаний; возникает возможность закрытия позиции. Пользователь или злоумышленник может запросить доступ к ресурсам какого-либо сетевого узла, с которым этот узел напрямую не связан. В таких случаях доступ осуществляется через какой-либо промежуточный узел, подключенный к обоим узлам или даже через несколько промежуточных узлов.

В условиях сети весьма непросто точно определить, откуда именно пришел запрос на доступ, особенно если захватчик приложит немного усилий к тому, чтобы скрыть это – в этом проявляется слабая защищенность линии связи [6]. Сеть отличается от той же системы тем, что захватчик в ней намерен включать телефонную линию, по которой данные передаются между узлами.

После этого можно транслировать телефонную линию, кабельные спутниковые каналы.

Основываясь на оценке рисков для безопасности компьютерных сетей, можно сделать выводы о свойствах и атрибутах, которые потребуются компании для систем интернет-безопасности.

1. Идентификация защищаемых ресурсов, т.е. присвоение защищаемым ресурсам идентификаторов – уникальных признаков, по которым в дальнейшем система производит аутентификацию.

2. Аутентификация защищаемых ресурсов, т.е. установление их подлинности на основе сравнения с эталонными идентификаторами.

3. Применение парольной защиты ресурсов.

4. Разграничение доступа пользователей к КС.

5. Разграничение доступа пользователей по операциям (чтение, запись, модификация и т. п.) над ресурсами (программы, файлы, каталоги, диски, сервера и т. д.) с помощью программных средств администрирования.

6. Регистрация событий: вход пользователя в сеть, выход из сети, нарушение прав доступа к защищаемым ресурсам и т. д.

7. Реакция на факты нарушения прав доступа к защищаемым ресурсам сети несанкционированного подключения к КС.

8. Обеспечение защиты информации при проведении ремонтно-профилактических работ.

Литература

1. Ганиев С.К., Каримов М.М. Вопросы оптимального сегментирования топологии локальных компьютерных сетей // Проблемы информатики и энергетики. 2001. № 2.

2. Коноваленко С.А., Королев И.Д., Симонов А.В. Оценка существующих средств анализа защищенности информационных систем // Наука вчера, сегодня, завтра. 2016. № 10 (32).

3. Коноваленко С.А., Королев И.Д. Выявление уязвимостей информационных систем // Инновации в науке. 2016. № 9 (58).

4. Лавров А.А., Лисс А.Р., Яновский В.В. Мониторинг и администрирование в корпоративных вычислительных сетях. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2013.

5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 4 изд., доп. и перераб. СПб.: Нарва, 2015.

6. Широчин В.П., Мухин В.Е., Кулик А.В. Вопросы проектирования средств защиты информации в компьютерных системах и сетях. Киев: ВЕК», 2016.