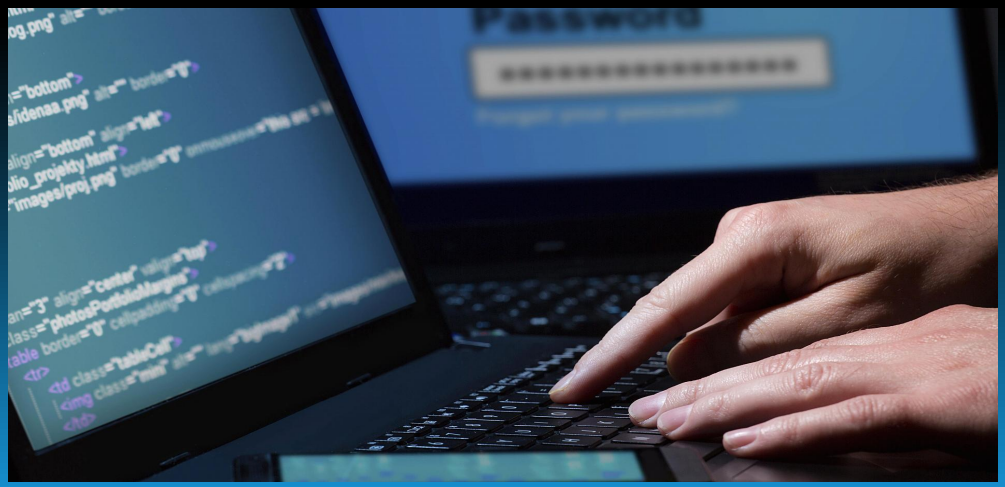
ЗАЩИТА ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Проведение финансовых операций с использованием Интернета, заказ товаров и услуг, использование кредитных карточек, доступ к закрытым информационным ресурсам, передача телефонных разговоров требуют обеспечения соответствующего уровня безопасности.

Конфиденциальная информация, которая передается по сети Интернет, проходит через определенное количество маршрутизаторов и серверов, прежде чем достигнет пункта назначения.



Принципы защиты информации

Проблемы безопасности передачи можно разделить на четыре основных типа:

- перехват информации - целостность информации сохраняется, но ее конфиденциальность нарушена;
- модификация информации - исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;
- подмена авторства информации;
- перехват сообщения с его изъятием.

Обычно маршрутизаторы не отслеживают проходящие сквозь них потоки информации, но возможность того, что информация может быть перехвачена, существует. Более того, информация может быть изменена и передана адресату в измененном виде. К сожалению, сама архитектура сети Интернет всегда оставляет возможность для недобросовестного пользователя осуществить подобные действия

Характеристики безопасность системы:

1. Аутентификация - это процесс распознавания пользователя системы и предоставления ему определенных прав и полномочий.
2. Целостность - состояние данных, при котором они сохраняют свое информационное содержание и однозначность интерпретации в условиях различных воздействий
3. Секретность - предотвращение несанкционированного доступа к информации.

Криптография

Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию
можно только при наличии ключа.

В основе шифрования лежат два основных понятия: алгоритм и ключ. Алгоритм - это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Зашифрованное послание может быть интерпретировано только с помощью ключа. Очевидно, чтобы зашифровать послание, достаточно алгоритма.

Электронная цифровая подпись

Передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют контр ольной суммой, или дайджестом сообщения. Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений.

Аутентификация

Аутентификация является одним из самых важных компонентов. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдает.

При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передает управление серверу аутентификации.

Защита сетей

Для защиты корпоративных информационных сетей используются брандмауэры. Брандмауэр - это система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую.

Заключение.

В данной работе мною были рассмотрены проблемы защиты информации в глобальной сети Internet. Проблема эта была и остается актуальной по сей день, так как никто еще не может гарантировать на сто процентов того, что ваша информация будет защищена. Разумеется в данной работе рассмотрена лишь часть проблемы Проведенные исследования показывают, что разработано множество способов защиты информации: разграничение доступа, защита при помощи паролей, шифрование данных и.т.п. Однако, несмотря на все это, до сих пор мы то и дело слышим о взломах хакерами различных серверов и компьютерных систем. Это говорит о том, что проблема защиты информации еще не решена и на ее решение будет потрачено множество сил и времени.