**Лекция №11. Защита информации в Интернет. Криптография и Интернет.**

**Цель лекции:** познакомиться с технологией шифрования (криптография) важной информации для защиты ее от изменений и неавторизованного доступа и изучить способы закодирования исходного текста (алгоритмы шифрования)

**Содержание лекции:** криптография. шифрование с симметричным и асимметричным ключом.

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. Однако использование ключа при шифровании предоставляет два существенных преимущества. Во-первых, можно использовать один алгоритм с разными ключами для отправки посланий разным адресатам. Во-вторых, если секретность ключа будет нарушена, его можно легко заменить, не меняя при этом алгоритм шифрования. Таким образом, безопасность систем шифрования зависит от секретности используемого ключа, а не от секретности алгоритма шифрования. Многие алгоритмы шифрования являются общедоступными. 44 Количество возможных ключей для данного алгоритма зависит от числа бит в ключе. Например, 8-битный ключ допускает 256 (28) комбинаций ключей. Чем больше возможных комбинаций ключей, тем труднее подобрать ключ, тем надежнее зашифровано послание. Так, например, если использовать 128- битный ключ, то необходимо будет перебрать 2128 = 1040 ключей, что в настоящее время не под силу даже самым мощным компьютерам. Важно отметить, что возрастающая производительность техники приводит к уменьшению времени, требующегося для вскрытия ключей, и системам обеспечения безопасности приходится использовать все более длинные ключи, что, в свою очередь, ведет к увеличению затрат на шифрование. Поскольку столь важное место в системах шифрования уделяется секретности ключа, то основной проблемой подобных систем является генерация и передача ключа. Существуют две основные схемы шифрования: симметричное шифрование (его также иногда называют традиционным или шифрованием с секретным ключом) и шифрование с открытым ключом (иногда этот тип шифрования называют асимметричным). При симметричном шифровании отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные. При симметричном шифровании используются ключи небольшой длины, поэтому можно быстро шифровать большие объемы данных. Симметричное шифрование используется, например, некоторыми банками в сетях банкоматов. Однако симметричное шифрование обладает несколькими недостатками. Во-первых, очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей. Во-вторых, для каждого адресата необходимо хранить отдельный секретный ключ. В третьих, в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом. В схеме шифрования с открытым ключом для шифрования послания используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго - расшифровывается. Таким образом, требуемой безопасности можно добиться, сделав первый ключ общедоступным (открытым), а второй ключ хранить только у получателя (закрытый, личный ключ). В таком случае любой пользователь может зашифровать послание при помощи открытого ключа, но расшифровать послание способен только обладатель личного ключа. При этом нет необходимости заботиться о безопасности передачи открытого ключа, а для того чтобы пользователи могли обмениваться секретными сообщениями, достаточно наличия у них открытых ключей друг друга. Недостатком асимметричного шифрования является необходимость использования более длинных, чем при симметричном шифровании, ключей для обеспечения эквивалентного уровня безопасности, что сказывается на вычислительных ресурсах, требуемых для организации процесса шифрования. 45 Криптография (от греч. Cryptos- тайный) - это наука и технология шифрования важной информации для защиты ее от изменений и неавторизованного доступа. Криптография служит не только для перевода текстов в нечитаемую зашифрованную форму, но позволяет также решить задачи аутентификации и идентификации пользователей при работе их в Сети. Криптография является основой безопасных коммуникаций. Следует отметить, что в Сети мы общаемся не только с людьми, но и с различными службами. Например, когда мы собираемся скачать с какого-либо сервера программу, нам тоже важно знать, что данный сервер принадлежит именно фирме-разработчику, а не фирме-пирату, которая может заразить ваш компьютер вирусом. Послание можно зашифровать и частным, и публичным ключом, а расшифровать только вторым ключом из пары. То есть послание, зашифрованное частным ключом, можно расшифровать только публичным, и наоборот. Частный ключ известен только владельцу, и его нельзя никому передавать, в то время как публичный ключ распространяется открыто всем корреспондентам. Пару ключей - частный и публичный - можно использовать как для решения задач аутентификации, так и секретности (конфиденциальности). Для того, чтобы обеспечить конфиденциальный обмен сообщениями в переписке двух лиц, необходимо иметь две пары ключей. При шифровании с помощью ключевой пары у вас нет необходимости рассылать свой публичный ключ всем корреспондентам. Гораздо удобнее выложить этот ключ в Сети на сервере с открытым доступом. Тогда каждый может скачать данный ключ и послать вам секретное сообщение, которое не прочтет никто кроме вас. Шифрование с симметричным и асимметричным ключом. Следует отметить, что алгоритм асимметричного шифрования сильно проигрывает алгоритму симметричного шифрования в плане эффективности, поэтому многие существующие системы шифрования используют комбинацию асимметричной и традиционной симметричной систем шифрования. Шифрование с открытым ключом используется для передачи симметричного ключа, который служит непосредственно для шифрования передаваемой информации.