76 Защита информации, передаваемой по открытым сетям

Безопасность (security) или, точнее, кибербезопасность (cybersecurity) -- в данном контексте, обеспечение защиты информации, передаваемой по открытым для прослушивания сетям.

Еще более общее чем сетевой экран понятие.

Задачи, решаемые в рамках обеспечения безопасности:

1. *Аутентификация* -- в данном контексте, обеспечение гарантии, что сообщение пришло от того, от кого его ожидают. Как правило, заключается в манипулировании с ключами. Алгоритмы: PSK, RSA и другие.

2. *Целостность* (integrity) -- обеспечение гарантии, что при пересылке сообщение не было повреждено и не было подменено. Как правило, заключается в подсчете значений хэш-функций. Алгоритмы: MD5 и SHA-256 и другие.

3. *Конфиденциальность* (confidentiality) -- обеспечение гарантии, что перехваченное сообщение не может быть прочитано. Как правило, заключается в шифровании данных. Алгоритмы: 3DES, AES и другие.

Как вариант, возможна маскировка конфиденциальных данных под неконфиденциальные, выражающаяся в различных алгоритмах *стеганографии* (steganography).

Во многие алгоритмы для формирования доверительных отношений между абонентами (security associations) заложено использование *цифровых подписей* (digital signatures) или *цифровых сертификатов* (digital certificates).

При этом гарантом ответственности (nonrepudiation) может выступать третья сторона, которой доверяют обе взаимодействующие стороны.

Современные тенденции в области безопасности компьютерных сетей сводятся к формированию так называемых *виртуальных частных сетей* -- VPNs (Virtual Private Networks), охватывающих взаимодействующие станции.

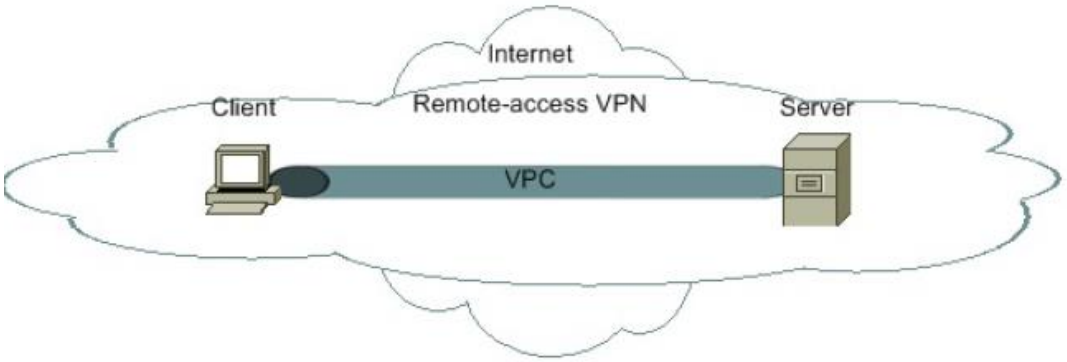
При этом взаимодействие осуществляется по формируемым особым образом (с целью максимальной защиты) *виртуальным частным каналам* -- VPCs (Virtual Private Channels), которые на практике обычно представляют

собой защищенные туннели, проложенные через открытые для прослушивания сети.

Все VPNs можно разделить на два типа:

1. Site-to-site -- в рядовом случае связывают одноранговые шлюзы и являются статическими (например, IPsec VPNs).

2. Remote-access -- в рядовом случае обеспечивают подключение удаленных пользователей, создаются динамически и базируются на клиент-серверной модели (например, TLS VPNs).



При администрировании, существуют две основополагающие политики обеспечения безопасности:

1. Разрешено все (по умолчанию), что не запрещено (явно).

2. Запрещено все, что не разрешено.

В настоящее время наиболее оправданным признан второй вариант.

// далее всякие стандарты и мб это не надо

Вопросы компьютерной безопасности, в том числе сетевой, как известно, находятся под контролем государства.

Ключевые стандарты Беларуси:

СТБ 34.101.1-2004 (ИСО/МЭК 15408-9) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

СТБ 34.101.2-2004 (ИСО/МЭК 15408-2:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

СТБ 34.101.3-2004 (ИСО/МЭК 15408-3:1999) «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности».

СТБ 34.101.4-2004 «Информационные технологии. Методы и средства безопасности. Профиль защиты электронной почты предприятия».

СТБ П 34.101.8-2003 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».

СТБ 34.101.11 -2004 «Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети».

СТБ П 34.101.14-2004 «Информационные технологии. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств маршрутизатора для использования в демилитаризованной зоне корпоративной сети»

СТБ 34.101.30-2007 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация».

СТБ 1176.1-99 «Информационная технология. Криптографическая защита информации. Функция хэширования».

СТБ 1176.2-99 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверка электронной цифровой подписи».

СТБ ГОСТ Р 50922-2000 «Защита информации. Основные термины и определения»