## 8.4. Механизмы безопасности информации, их виды

Для реализации средств безопасности в информационных технологиях от несанкционированных воздействий, оказываемых на вычислительную технику и каналы связи (прочтение информации в сетевых пакетах, изменение содержания полей данных в сетевых пакетах, подмена отправителя/получателя), наибольшее распространение получили криптографические средства защиты.

**Механизм криптографической защиты** на сетевом уровне корпоративной вычислительной сети строится на сертифицированных ФАПСИ (Федеральное агентство правительственной связи и информации) - аппаратно-программных комплексах, которые обеспечивают защиту информации.

Сущность криптографии заключается в следующем.

Готовое к передаче сообщение (данные, речь или графическое сообщение того или иного документа) обычно называется открытым, исходным или незащищенным текстом или сообщением. В процессе передачи такого сообщения по незащищенным каналам связи оно может быть легко перехвачено или отслежено заинтересованным лицом посредством его умышленных или неумышленных действий. Для предотвращения несанкционированного доступа к этому сообщению оно зашифровывается и тем самым преобразуется в шифрограмму или закрытый текст. Когда же санкционированный пользователь получает сообщение, он дешифрует или раскрывает его посредством обратного преобразования криптограммы, вследствие чего получается исходный открытый текст.

Метод преобразования в криптографической системе определяется используемым специальным алгоритмом. Работа такого алгоритма определяется уникальным числом или битовой последовательностью, обычно называемой шифрующим ключом.

Каждый используемый ключ может производить различные шифрованные сообщения, определяемые только этим ключом. Для большинства систем закрытия схема генератора ключа может представлять собой либо набор инструкций, команд, либо часть или узел аппаратуры (hardware), либо компьютерную программу (software), либо все эти модули одновременно. Однако в любом случае процесс шифрования / дешифрования единственным образом определяется выбранным специальным ключом. Таким образом, чтобы обмен зашифрованными сообщениями в информационных технологиях проходил успешно, отправителю и получателю необходимо знать правильную ключевую установку и хранить ее в тайне.

Следовательно, стойкость любой системы закрытой связи определяется степенью секретности используемого в ней ключа. Тем не менее, этот ключ должен быть известен другим пользователям сети так, чтобы они могли свободно обмениваться зашифрованными сообщениями. В этом случае криптографические системы также помогают решить проблему аутентификации принятой информации, т. к. подслушивающее лицо, пассивным образом перехватывающее сообщение, будет иметь дело только с зашифрованным текстом.

В то же время истинный получатель, приняв сообщение, закрытое известным ему и отправителю ключом, будет надежно защищен от возможной дезинформации.

В информационных технологиях используются различные типы шифрования:

| | |
|---|---|
| Симметричное шифрование основывается на использовании одного и того же секретного ключа для шифрования и дешифрования | Асимметричное шифрование характеризуется тем, что для шифрования используется один ключ, являющийся общедоступным, а для дешифрования - другой, являющийся секретным. При этом знание общедоступного ключа не позволяет определить секретный ключ |

Наряду с шифрованием в информационных технологиях используются следующие механизмы безопасности,

1. **Механизм цифровой (электронной) подписи** в информационных технологиях основывается на алгоритмах ассиметричного шифрования и включает две процедуры: формирование подписи отправителем и ее опознание (верификацию) получателем. Первая процедура обеспечивает шифрование блока данных или его дополнение криптографической контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знание которого достаточно для опознавания отправителя.
2. **Механизмы контроля доступа** осуществляют проверку полномочий объектов информационной технологии (программ и пользователей) на доступ к ресурсам сети. В основе контроля доступа к данным лежит система разграничения доступа специалистов информационной технологии к защищаемой информации.

   Реализация систем разграничения доступа представляет собой программу, которая ложится всем своим телом на операционную систему и должна закрыть при этом все входы в операционную систему, как стандартные, так и всевозможные нестандартные. Запуск системы разграничения доступа осуществляется на стадии загрузки операционной системы, после чего вход в систему и доступ к ресурсам возможен только через систему разграничения доступа. Кроме этого, система разграничения доступа содержит ряд автономных утилит, которые позволяют настраивать систему и управлять процессом разграничения доступа.

   Система разграничения доступа контролирует действия субъектов доступа по отношению к объектам доступа и, на основании правил разграничения доступа, может разрешать и запрещать требуемые действия.

   Для успешного функционирования системы разграничения доступа в информационных технологиях решаются следующие задачи:

   - невозможность обхода системы разграничения доступа действиями, находящимися в рамках выбранной модели;
   - гарантированная идентификация специалиста информационной технологии, осуществляющего доступ к данным (аутентификация пользователя).
3. **Система регистрации и учета информации** является одним из эффективных методов увеличения безопасности в информационных технологиях. Система регистрации и учета, ответственная за ведение регистрационного журнала, позволяет проследить за тем, что происходило в прошлом, и соответственно перекрыть каналы утечки информации. В регистрационном журнале фиксируются все осуществленные или неосуществленные попытки доступа к данным или программам. Содержание регистрационного журнала может анализироваться как периодически, так и непрерывно.

В регистрационном журнале ведется список всех контролируемых запросов, осуществляемых специалистами ИТ, а также учет всех защищаемых носителей информации с помощью их маркировки, с регистрацией их выдачи и приема.

4. **Механизмы обеспечения целостности информации** применяются как к отдельному блоку, так и к потоку данных. Целостность блока является необходимым, но не достаточным условием целостности потока. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока данных, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.
5. **Механизмы аутентификации** подразделяются на одностороннюю и взаимную аутентификацию. При использовании односторонней аутентификации в ИТ один из взаимодействующих объектов проверяет подлинность другого. Во втором случае - проверка является взаимной.
6. **Механизмы подстановки трафика или подстановки текста** используются для реализации службы засекречивания потока данных. Они основываются на генерации объектами ИТ фиктивных блоков, их шифровании и организации передачи по каналам связи. Тем самым нейтрализуется возможность получения информации об информационной технологии и обслуживаемых ее пользователей посредством наблюдения за внешними характеристиками потоков информации, циркулирующих по каналам связи.
7. **Механизмы управления маршрутизацией** обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по скомпрометированным (небезопасным), физически ненадежным каналам.

**Механизмы арбитража** обеспечивают подтверждение характеристик данных, передаваемых между объектами информационных технологий, третьей стороной (арбитром). Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики.