Инженерно-технические методы и средства защиты информации

Это физические объекты, механические, электрические и электронные устройства, элементы конструкций зданий, средства пожаротушения и др.

обеспечивают:

- защиту территории и помещения КС от проникновения
- защиту аппаратных средств и носителей информации
- предотвращение возможного удаленного видеонаблюдения, подслушивания
- предотвращение возможностей перехвата ПЭМИН
- организацию доступа в помещении КС сотрудников
- контроль за режимом работы персонала кс
- контроль над перемещением сотрудников КС в различных производственных зонах
- противопожарную защиту помещений
- минимизацию материального ущерба от потерь информации из-за стихийных бедствий и техногенных аварий.

Методы и средства защиты информации от утечки по каналам ПЭМИН

1. Снижение уровня излучений сигналов в аппаратных средствах КС
2. Увеличение мощности помех в частотных диапазонах (генераторы сигналоподобных помех или шума)

Перспективные методы и средства защиты информации в КС от утечки по каналам ПЭМИН

- элементная база с более малым уровнем информационных сигналов
- замена электро цепей на оптоволокно
- локальное экранирование узлов технических средств
- включение в состав устройств предварительного шифрования обр. информации.

Аппаратно-программные средства защиты информации

1. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
2. Системы шифрования дисковых данных.
3. Системы шифрования данных, передаваемых по сетям.
4. Системы аутентификации электронных данных.
5. Средства управления криптографическими ключами.

7. Системы идентификации и аутентификации пользователей .

Применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы.

Общий алгоритм работы:

1. получить от пользователя информацию, удостоверяющую его личность
2. проверить ее подлинность
3. предоставить (или не предоставить) этому пользователю возможность работы с системой.

Типы выбора информации

- **Традиционные** - секретная информация пользователя (пароль, секретный ключ, персональный идентификатор и т.п.); пользователь должен запомнить эту информацию или же для нее могут быть применены специальные средства хранения;
- **Биометрические** - физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

2. Системы шифрования дисковых данных

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая ***криптографией*** [от греч. ***kryptos*** - скрытый и ***grapho*** - пишу].

Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков.

К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt.

По способу функционирования системы шифрования дисковых данных делят на два класса

1. **системы "прозрачного" шифрования** - (шифрования "на лету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя.

   Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

2. **системы, специально вызываемые для осуществления шифрования** - это утилиты, которые необходимо специально вызывать для выполнения шифрования.
   Например, архиваторы со встроенными средствами парольной защиты.

   Большинство систем, предлагающих установить пароль на документ, не шифрует информацию, а только обеспечивает запрос пароля при доступе к документу.

К таким системам относится MS Office, 1С и многие другие.

3. Системы шифрования данных, передаваемых по сетям

1 ***канального шифрования*** защищается вся информация, передаваемая по каналу связи, включая служебную .

«+» повышению производительности системы за счет использования аппаратные средства

«-»

- сложность маршрутизации сетевых пакетов и необходимость расшифрования данных в устройствах промежуточной коммуникации (шлюзах, ретрансляторах и т.п.);
- приводит к появлению статистических закономерностей в шифрованных данных, влияет на надежность защиты и ограничивает использование криптографических алгоритмов.

- **2. Оконечное (абонентское) шифрование** позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами.

  Защищено содержание сообщений, вся служебная информация - открыта.

  Недостаток - возможно анализировать информацию о структуре обмена сообщениями (например об отправителе и получателе, о времени и условиях передачи данных), а также об объеме передаваемых данных

4. Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе.

Для аутентификации данных применяют код аутентификации сообщения (**имитовставку**) или **электронную подпись**.

Имитовставка

Это шифрование открытых данных с помощью секретного ключа и передается по каналу связи в конце зашифрованных данных. (симметричное шифрование)

Проверяется получателем, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.

Электронная цифровая подпись (ЭЦП)

Это относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. (ассиметричное шифрование).

Отправитель формирует цифровую подпись, используя секретный ключ отправителя.

Получатель проверяет подпись, используя открытый ключ отправителя.

5. Средства управления криптографическими ключами

виды функций управления ключами:

1. генерация
2. хранение
3. распределение ключей

1. Генерация ключей

В симметричных криптосистемах используются аппаратные и программные средства генерации случайных чисел.

В асимметричных криптосистемах - ключи должны обладать определенными математическими свойствами.

2. Хранение

Организация безопасного хранения, учета и удаления ключевой информации.

Для безопасности применяют шифрование с помощью других ключей. (иерархия ключей). В иерархию ключей обычно входит главный ключ (т.е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Генерация и хранение мастер-ключа является критическим вопросом криптозащиты.

3. Распределение

Самый ответственный процесс в управлении ключами. Он должен гарантировать скрытность распределяемых ключей, оперативность и точность.

Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.