

Аппаратные методы защиты информации

Работу выполнила:
Ярыгина Ольга,
Группа МНБ 1601-01-00

Инженерно-техническая защита (ИТЗ) — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Инженерно-техническая защита

КЛАССИФИКАЦИЯ ИТЗ по используемым средствам

ФИЗИЧЕСКИЕ

Устройства, инженерные сооружения и организационные меры, затрудняющие или исключающие проникновение злоумышленников к источникам конфиденциальной информации

АППАРАТНЫЕ

Механические, электрические, электронные и др. устройства, предназначенные для защиты информации от утечки и разглашения и противодействия техническим средствам промышленного шпионажа

ПРОГРАММНЫЕ

Система специальных программ, включаемых в состав общего и специального обеспечения, реализующих функции защиты информации и сохранения целостности и конфиденциальности

КРИПТОГРАФИЧЕСКИЕ

Технические и программные средства шифрования

КОМБИНИРОВАННЫЕ

Совокупная реализация аппаратных и программных средств и криптографических методов защиты информации

Аппаратные средства защиты

информации:

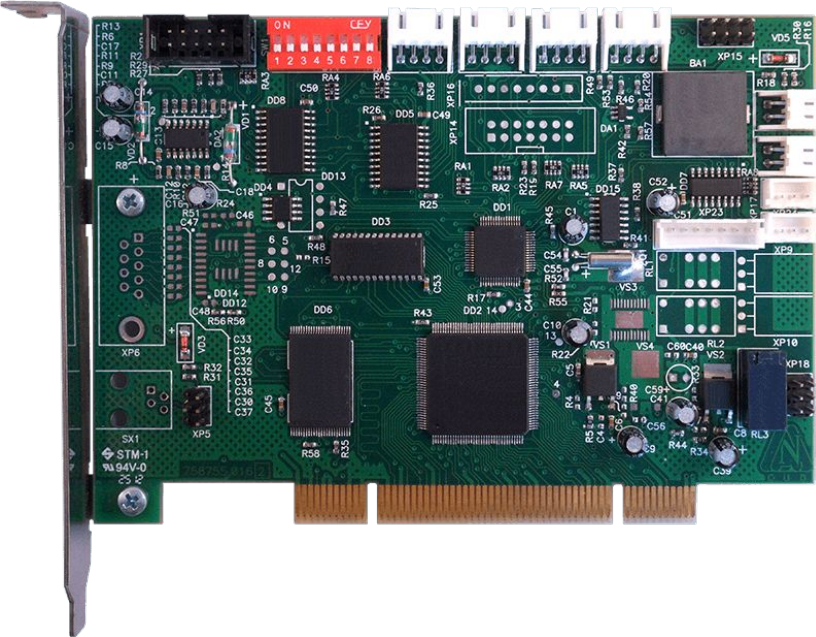
1. Специальные регистры для хранения реквизитов защиты;
2. Генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;
3. Устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
4. Специальные биты секретности, значение которых определяет уровень секретности информации, которой принадлежат данные биты;
5. Схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

Аппаратные устройства криптографической защиты

- это такие устройства, представляющие собой платы, модули и даже отдельные системы, выполняющие различные алгоритмы шифрования.



«КРИПТОН-ЗАМОК»



- Идентификация пользователя до запуска BIOS компьютера;
- Разграничение и контроль доступа пользователей к ПЭВМ;
- Разграничение доступа к аппаратным ресурсам ПЭВМ;
- Управление шифраторами;
- Блокировка компьютера при НСД

Аппаратные средства защиты информации

Классификация

<i>По функциональному назначению</i>	<ol style="list-style-type: none">1. Средства обнаружения2. Средства поиска3. Детальных измерений4. Активного противодействия5. Пассивного противодействия
<i>По техническим возможностям</i>	<ol style="list-style-type: none">1. Общего назначения2. Профессиональные комплексы

Примером сложного современного поисково-обнаружительного профессионального комплекса можно назвать комплекс «Дельта», который обеспечивает достоверное обнаружение практически любых из имеющихся в продаже радиомикрофонов, радио-стетоскопов, сетевых и телефонных передатчиков, в том числе и с инверсией спектра; автоматическое определение места расположения микрофонов в объеме контролируемого помещения

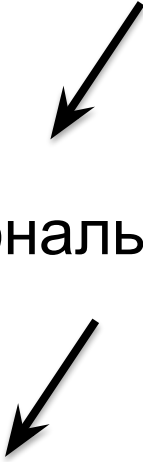


Электронный ключ eToken - персональное средство авторизации, аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью



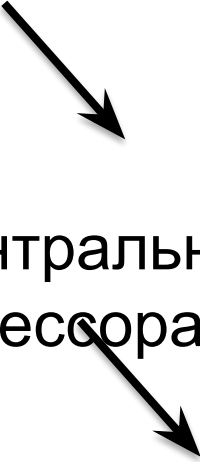
- В особую группу выделяются аппаратные средства защиты ЭВМ и коммуникационных систем на их базе.

- Аппаратные средства защиты применяются:



в персональных
ЭВМ

в контроллерах ввода-вывода



в центральных
процессорах

в внешних ЗУ и т.
п.

Работа любых электронных устройств сопровождается **электромагнитными излучениями.**

Источники электромагнитных излучений:

1. компьютеры;
2. активные элементы локальных сетей;
3. кабели.

Программно-аппаратные брандмауэры -
специальные комплексы, созданные для
защиты от несанкционированного
проникновения .

В простейшем случае брандмауэром может служить
фильтрующий маршрутизатор



□ Для автоматического уничтожения данных используются специальные модули, которые могут встраиваться в системный блок или исполняться как внешнее устройство с установленными в нем накопителями информации. Команда на полное уничтожение данных для таких аппаратов подается обычно дистанционно со специального брелока или с любых датчиков, которые вполне могут отслеживать как вторжение в помещение, так и несанкционированный доступ к устройству, его перемещение или попытку отключения питания.

□ Информация в таких случаях уничтожается одним из двух способов:

- физическое разрушение накопителя (обычно химическими средствами)
- стирание информации в служебных областях дисков

Вывод

Аппаратные средства защиты информации, к которым относятся различные технические устройства, системы и сооружения, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа, **более эффективны и надежны.**

Именно поэтому они применяются тогда, когда речь идет, например, о военных секретах или о больших суммах денег.

**Спасибо за
внимание!**